Building a More Secure and Prosperous Texas

A Report from the
TEXAS CYBERSECURITY, EDUCATION, AND
ECONOMIC DEVELOPMENT COUNCIL

Updated Version

December 1, 2012

About the

Texas Cybersecurity, Education, and Economic Development Council

In 2011, the 82nd Texas Legislature passed and the Governor signed Senate Bill 988, which authorized the creation of the Cybersecurity, Education, and Economic Development Council. The legislation directed the Department of Information Resources to appoint a nine-member council from across government, academia, and industry. The Council is to provide recommendations to the Texas Legislature regarding ways to 1) improve the infrastructure of the state's cybersecurity operations with existing resources and through partnerships between government, business, and institutions of higher education; and 2) examine specific actions to accelerate the growth of cybersecurity as an industry in Texas.

Contents

Executive Summary

With the advancement of technology and the proliferation of computer systems and networks, cybersecurity threats to Texas government and industries are evolving in complexity and severity and growing in number, outpacing Texas organizations' ability to protect the state's cyber environment. This puts the private information of Texas citizens, including that of children, at risk. Additionally, the risk extends to the intellectual property of Texas businesses and to the security of the state.

In fiscal year 2011, the 82nd Texas Legislature passed and the Governor signed Senate Bill (SB) 988, which authorized the creation of the Texas Cybersecurity, Education, and Economic Development Council (Council). The Council was chartered to provide recommendations to the state leadership regarding ways to 1) improve the infrastructure of the state's cybersecurity operations, both with existing resources and through partnerships between government, business, and institutions of higher education; and 2) examine specific actions to accelerate the growth of cybersecurity as an industry in the state.

The Council examined three areas of importance to the state: its cybersecurity infrastructure, its cybersecurity industry, and the cybersecurity educational needs for fostering a vigilant and effective cyber culture. A detailed discussion of these areas is provided later in this document. As a result of the examination, the Council found that Texas must establish a statewide focus for its cyber environment. This focus would include Texas business and public leaders in collaborative efforts to identify and mitigate risks and threats to Texas citizens and to spur innovation in the cyber environment. The Council recommends:

1. **Establishing a Texas Coordinator of Cybersecurity within the Office of the Governor** to provide a strategic direction to bring government and business leaders together as partners in securing the state's infrastructures and developing a strategy and plan to promote the cybersecurity industry within the state.
2. **Establishing the Business Executives for Texas Security (BETS) partnership** to bring public- and private-sector leaders and cybersecurity practitioners together to form a framework for knowledge sharing and collaboration, making non-proprietary and industry-recognized best practices and solutions readily available for the collective improvement of cybersecurity across the state.
3. **Establishing a "Cyber Star" program** to foster improvement of cyber resiliency in both private and public infrastructures across the state and to increase public trust by establishing a baseline for responsible cyber operations.
4. **Adopting the Community Cyber Security Maturity Model as a statewide guide** for developing a viable and sustainable cybersecurity program and fostering a culture of cybersecurity throughout the state.
5. **Increasing the number of cybersecurity practitioners in Texas** to provide the expertise needed to grow cybersecurity investment and to protect the cyber assets of the state.

6. **Providing a consistent voice for industry** regarding cybersecurity policies in order to facilitate communication between the state and industry.
7. **Continuing investment in higher education cybersecurity programs** in order to attract students to the cybersecurity field, spur research and development, and encourage institutions of higher education to become leaders in cybersecurity within their own communities.
8. **Promoting collaboration, innovation, and entrepreneurship in cybersecurity** to facilitate the commercialization of university research and development and encourage the development of new businesses with innovative products and services in cybersecurity.
9. **Developing a comprehensive cybersecurity education pipeline through the BETS partnership** to introduce cybersecurity initiatives from K–PhD**.**
10. **Reviewing and sharpening the leadership role of the Texas Department of Information Resources (DIR)** in establishing a sustainable Cybersecurity Awareness Program for all Texans.

Introduction

Texas Economy and Critical Technology Infrastructures at Risk

Cybersecurity threats continue to evolve and are outpacing Texas organizations' ability to protect the state's cyber environment, compromising the physical safety, financial security, and privacy of Texas citizens. Public, non-profit, and commercial entities within the state are challenged to collaboratively identify and mitigate large-scale cyber events by national and international entities with intent and ability to cause critical outages, steal private information, or harm Texas government and business in other ways.

In response to the rapidly expanding Texas and national cyber threat landscape, the 82nd Texas Legislature took steps in 2011 to leverage public/private partnerships to examine the infrastructure of the state's cybersecurity operations. These operations include the administrative and technical measures taken to protect business against unauthorized access or attack, including preventing criminal or unauthorized use of electronic customer data. The effort is intended to produce strategies to accelerate the growth of cybersecurity as an industry within Texas. This includes both cybersecurity businesses that create and market security products and services, as well as those businesses with significant cybersecurity operations requirements. The goal is to encourage all industry members to call Texas "home."

The Texas Cyber Environment Today

The U.S. cyber environment is clearly at risk. From October 2011 through February 2012, more than 50,000 cyber-attacks on private and government networks were reported to the U.S. Department of Homeland Security, including 86 attacks against "critical infrastructure networks." These attacks, regardless of originating country, likely represent a small fraction of cyber-attacks carried out in the United States. It is important to note that cyber-attacks are not confined to the realm of cyberspace. A cyber-attack can also inhibit, intrude upon, or damage physical property such as machines, motors, and physical processes controlled by computers. Today, underlying control systems and technologies are converging due to the acceptance of Internet Protocol (IP) as the *de facto* method of linking these systems. Thus, the cyber environment includes a symbiotic relationship with virtually all public and private economic clusters because of the computers, software, telecommunications, and embedded control systems at the heart of critical infrastructure.

Texas organizations rely on the state's cyber environment to deliver many commercial, government, and education products and services to Texas' more than 26 million citizens. The Texas environment includes public organizations such as state agencies, higher education institutions, local governments, K–12 education, and emergency management districts, as well as private entities. This environment also encompasses for-profit and not-for-profit corporations, including faith-based organizations, 50+ U.S. Fortune 500 companies headquartered in Texas, and many U.S. and global firms with significant business operations in the state. Texas business must ensure it effectively and continuously protects the state's cyber environment in order to support the Texas economy.

The Texas cyber environment, including critical infrastructures such as water, energy, healthcare, banking, and transportation, is shared and governed by a myriad of Texas public and private organizations with differing organizational missions and regulatory requirements for privacy and security. Each organization is required to establish and maintain appropriate cybersecurity operations, processes, and technologies and hire trained, professional cybersecurity staff to protect their operations and the information entrusted to them by Texas citizens.

Looking Back: SIPAC Assessment of Texas Critical Infrastructure

The state's critical infrastructures were the subject of the 2001 State Infrastructure Protection Advisory Committee (SIPAC) assessment commissioned by the Texas Attorney General. SIPAC was charged to review Texas' critical infrastructures and make recommendations for protecting this portion of the Texas cyber environment.

The SIPAC report, released in 2002, focused on state agency, higher education, and emergency management. It proposed creating many strategic, tactical, and operational Texas homeland security and technology infrastructure protection capabilities for state critical infrastructures. The enhancements implemented as a result of SIPAC's recommendations included creating the Texas Department of Homeland Security. Additionally, the Texas Department of Information Resources (DIR) created plans, strategies, policies and related operations and services capabilities related to protection of critical technology infrastructures. Many Texas critical infrastructures are also now subject to compliance with federal government and industry security requirements that have influenced public and private organizations to invest in improving their cyber operations capabilities.

While SIPAC spurred statewide efforts, and further federal regulation has helped advance many of SIPAC's critical infrastructure goals, these efforts have neither extended to non-critical infrastructure portions of the state's cyber environment nor led to the coordination of protection activities between Texas public and private organizations.

Senate Bill 988 Charge and Council Analysis and Assessment

Fiscal year 2011 legislation, through Senate Bill (SB) 988, charged DIR with appointing nine members from across government, academia, and industry to form the Texas Cybersecurity, Education, and Economic Development Council. The Council is responsible for conducting an interim study and providing recommendations to DIR's Executive Director regarding ways to 1) improve the infrastructure of the state's cybersecurity operations with existing resources and through partnerships between government, business, and institutions of higher education; and 2) examine specific actions to accelerate the growth of cybersecurity as an industry in the state. The Council is required to submit its findings by December 1, 2012, to the

- DIR Executive Director
- Governor
- Lieutenant Governor
- Speaker of the House of Representatives
- Higher Education Committees of the Senate and House of Representatives

- Senate Committee on Economic Development
- House Technology Committee
- House Economic and Small Business Development Committee

The Council focused on analyzing the cybersecurity economic development context, cybersecurity education capabilities, and cyber operations for the state's cyber infrastructure environment, both public and private. In performing the analysis, the Council conducted an online survey of government and business organizations; analyzed DIR's database of state agency information resources survey responses; held face-to-face and "virtual" meetings with Texas and federal cybersecurity workforce, education, and training experts; and met with Texas and national cybersecurity infrastructure experts on emerging federal and private enterprise cybersecurity infrastructure trends. The Council performed a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis of statewide cybersecurity infrastructure, industry, and education capabilities.

The results of this analysis are below.

Strengths

- DIR has established a strong information security program for state agencies and is capable of taking on a greater leadership role in cybersecurity.
- Texas has a great track record in attracting new industry and providing a good environment for business operations.
- Texas has many current private-sector champions to support growth of the cybersecurity industry within Texas.
- Good models exist for successful metro area participation in cybersecurity programs and innovation centers ("Pockets of Excellence").
- Texas has 12 National Security Agency (NSA)/ Department of Homeland Security (DHS) Centers of Academic Excellence in Information Assurance Education and/or Research tied to higher education.
- Texas Administrative Code 202 provides a good framework for securing cyber infrastructure.

Weaknesses

- Both private- and public-sector organizations have developed internal cybersecurity activities that are often sub-optimized. Best practices are not shared.
- There is no centralized database for contacts and communications processes for organizations in Texas.
- Resources have not been quantified for cybersecurity activities.
- There is not an established forum for industry to participate with state government for enhancing cybersecurity in Texas.
- There is a general lack of awareness regarding securing the cyber infrastructure.
- There is an insufficient number of qualified, trained cybersecurity personnel to meet industry demand.

Opportunities

- There is an alignment of thought around cybersecurity by Texas industry and state government leaders.
- Best practices in cybersecurity activities can be shared and replicated (scalable).
- Cybersecurity awareness has increased at the federal level. Federal reports and other resources regarding cybersecurity, especially information, are becoming available.
- Cybersecurity training resources may be available from certain state agencies and higher education institutions. These existing resources can be harnessed to create a centralized repository of cybersecurity knowledge and skills in Texas.
- Media has begun covering major cybersecurity incidents.

Threats

- Sophistication of attackers is increasing (e.g., nation states, organized crime, hacktivists).
- The number and severity of cybersecurity exploits have increased.
- The nature of cybersecurity exploits has become more threatening (i.e., the scope of impact spans national security compromises, economic loss, terrorism, and the standard factors of nuisance and personal loss).
- Rapid advancements in technology (e.g., mobile computing, social networks, and cloud computing), coupled with a large population of computer users under-educated in cybersecurity awareness creates an environment ripe for major losses and damages caused by cybersecurity exploits.
- As critical infrastructure resources (e.g., energy and water) become increasingly dependent on computing networks for operations and maintenance, they also become potential targets for cybersecurity exploits. These critical infrastructure resources are, however, prerequisites for industry growth in Texas.

Council Call for Action

Texas must establish a statewide focus for the Texas cyber environment, one that extends beyond critical infrastructure networks to include Texas business and public leaders in collaborative efforts to identify and mitigate risks and threats to Texas citizens and to spur innovation in the cyber environment. The Council recommends Texas executive and legislative branches consider establishing a framework for designating oversight of cybersecurity coordination and for a sustainable private/public-sector partnership working jointly to improve the state's cybersecurity posture and to protect and enhance its economy. Texas must enable this framework for action by defining specific statewide authority, influencing adoption across non-government industry, creating special public-private partnerships, designating funding authority or sources for sustainability and growth, and considering impact of emerging cyber threats and cyber regulation challenges. This will allow Texas to continuously enhance statewide cybersecurity infrastructure and education capabilities and advance statewide cybersecurity economic development through business expansion, recruiting, and research and development commercialization efforts. These structures and processes are needed to ensure that Texas effectively and continuously designs, implements, and upgrades cybersecurity operations, hires and retains trained and capable cybersecurity workers

to manage the state's cyber risk, and creates statewide cybersecurity industry and cybersecurity industry opportunities.

Findings and Recommendations

To fulfill its charter, the Council explored findings and recommendations in three key areas:

- Texas' cybersecurity **infrastructure** was analyzed in an effort to develop recommendations that could lead to improving both the state's cybersecurity infrastructure and its ability to coordinate cybersecurity efforts among non-governmental elements within the state.
- **Industry**, a vital part of the cybersecurity environment, was examined from two standpoints—first from the perspective of how the security of cyber assets in the state's industries could be improved and, second, how more industry could be attracted to the state to spur greater economic development.
- The Council examined **education** from the perspective of both formal degree and certification programs as well as general awareness of cybersecurity issues within the state.

Advancing Cyber Secure Infrastructure in Texas

Findings

The cybersecurity strengths and opportunities that already exist within Texas demonstrate significant potential for advancing a more secure cyber infrastructure across the state. However, the weaknesses and threats identified during the Council's deliberations resulted in three significant findings that drove development of recommendations for infrastructure improvement.

There is no single lead office for cybersecurity coordination of policy and response in Texas. Although the Council deems DIR's Information Security Program for state agencies a major strength, and although Texas Government Code does, in fact, name DIR's Executive Director as the State Chief Information Officer, the powers and duties of that position outlined in the code, as well as those of DIR itself, are limited mostly to procurement and security oversight within state agencies and do little to generate and coordinate the partnerships between public and private entities that are necessary to the collective cybersecurity of Texas (*Texas Government Code, Sections 2054.0285, 2054.052 regarding duties and powers of the Executive Director and the Department of Information Resources*).

Lack of a coordinated cybersecurity effort across the state allows malicious cyber activities to outpace the development of a secure infrastructure to effectively counter those activities. To gather information about the current state of the cybersecurity infrastructure in Texas, the Council surveyed organizations throughout Texas. This effort uncovered a significant impediment to obtaining valid survey results across multiple sectors, namely the lack of an established statewide comprehensive contact list of cybersecurity leads for all levels of state, county, and municipal government along with major Internet service providers, other telecommunications companies, military installations, and critical infrastructure. This is a critical state deficiency affecting both proactive and reactive cybersecurity efforts, as well as potentially affecting other state operations.

The Council found several examples of innovation and cyber excellence in and around major metropolitan areas and military installations; however, these efforts are mostly localized rather than programs to expand to regional or statewide models. The commitment of cities such as San Antonio, whose elected leadership, Chamber of Commerce, businesses, military community, universities and colleges, and independent school districts have joined in a focused collective effort to increase cybersecurity education and awareness by leveraging opportunities in the areas of people, process, and technology have resulted in nationally recognized cybersecurity success. These models should be considered across the state. There are other examples of innovation and achievement in cybersecurity throughout Texas. For example, Figure 1 shows the list of NSA/DHS Centers of Academic Excellence in Information Assurance found in Texas.

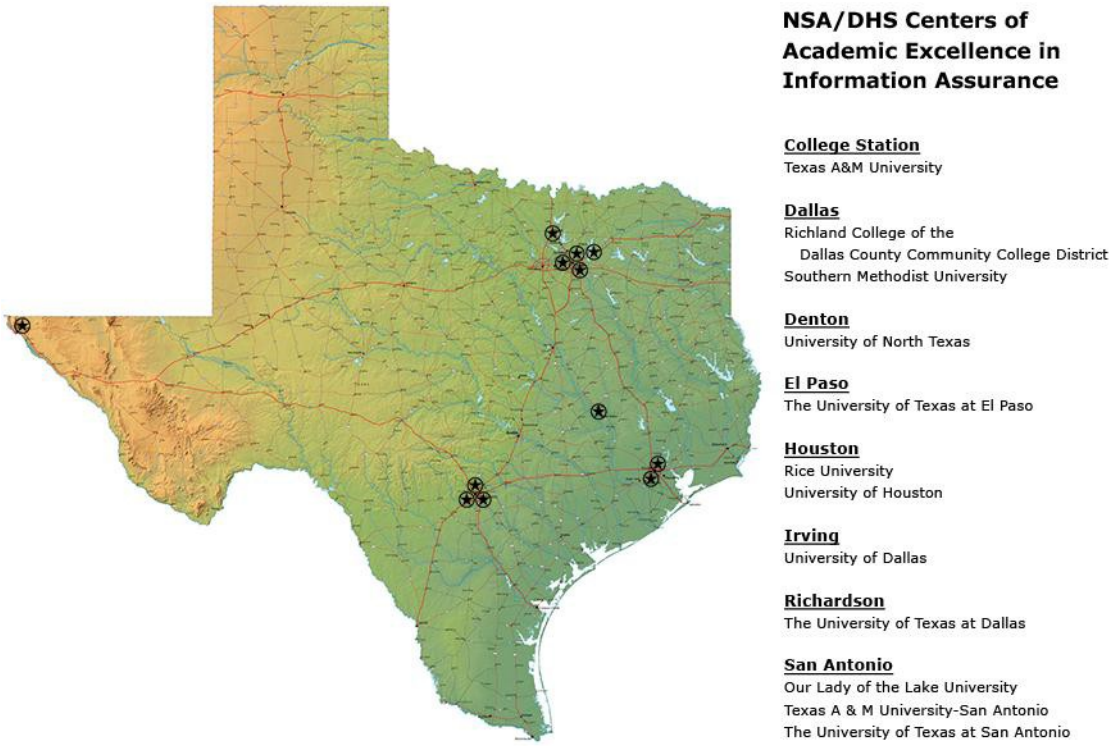


Figure 1. NSA/DHS Centers of Academic Excellence for Information Assurance in the State of Texas

Although these centers for advancement exist in Texas, a significant gap remains between the levels of resourcing that private industry expends for cybersecurity and the levels of resourcing available to state and local governments, school districts, and other non-profit entities. In most instances, the question is not whether to establish a cybersecurity program, but rather where to start. The absence of a generally accepted baseline against which less densely populated and rural communities, small businesses, non-profit organizations, utility districts, and school districts can use to measure progress toward cyber maturity leaves these organizations, and by extension the citizens and customers they serve, persistently vulnerable.

Recommendations

Whether large or small, whether mature or just getting started, Texas' cybersecurity infrastructure is an interconnected chain of systems that is only as strong as the weakest link. The Council proposes five strategic actions for advancing Texas' cyber secure critical infrastructure:

- Establish a Texas Coordinator of Cybersecurity within the Office of the Governor.
- Establish the Business Executives for Texas Security (BETS) Partnership.
- Establish a "Cyber Star" program to foster improvement of cyber resiliency in both private and public infrastructure in the state as well as increasing public trust.
- Adopt the Community Cyber Security Maturity Model (CCSMM) as a statewide guide for developing processes leading to a state of cyber maturity.
- Expand and strengthen DIR's duties and powers.

Establish a Texas Coordinator of Cybersecurity within the Office of the Governor.

Improving cybersecurity for a state the size and complexity of Texas requires a heightened synergy of effort as well as different leadership expectations to address the question of "who's in charge" when it comes to cybersecurity.

While DIR has performed well in this role and should continue to perform this function for the diverse agencies and departments of state government, Texas requires a charismatic and empowered leader who has the support of the Office of the Governor and possesses the authority and the initiative to bring influential government and business leaders together as partners in the interest of a statewide cybersecurity agenda. Cybersecurity is pervasive and impacts virtually all industries and government sectors while at the same time representing an overlooked industry cluster with a unique opportunity for wealth creation through concerted research, development, and commercialization efforts.

This recommendation does not come without some historic challenges. Creating new functional organizational coordinators or "czars" often fails because they are given great responsibilities but few authorities to necessitate collaboration across diverse agencies and departments as well as the private sector and higher education.

Improved collaboration between public and private sectors on advancing the collective cybersecurity of the state requires support of executive leadership. To best ensure success, the Council recommends the active participation of the Office of the Governor to encourage proactive engagement from other senior leaders of public and private sectors. Economic development initiatives will also benefit from executive leadership in convening the marketplace and exploring opportunities in partnership with the Texas Enterprise Fund, the Texas Emerging Technology Fund, and emerging insurance and risk management markets. Figure 2 depicts the central role the Texas Coordinator of Cybersecurity would play in synchronizing cybersecurity efforts in the state.

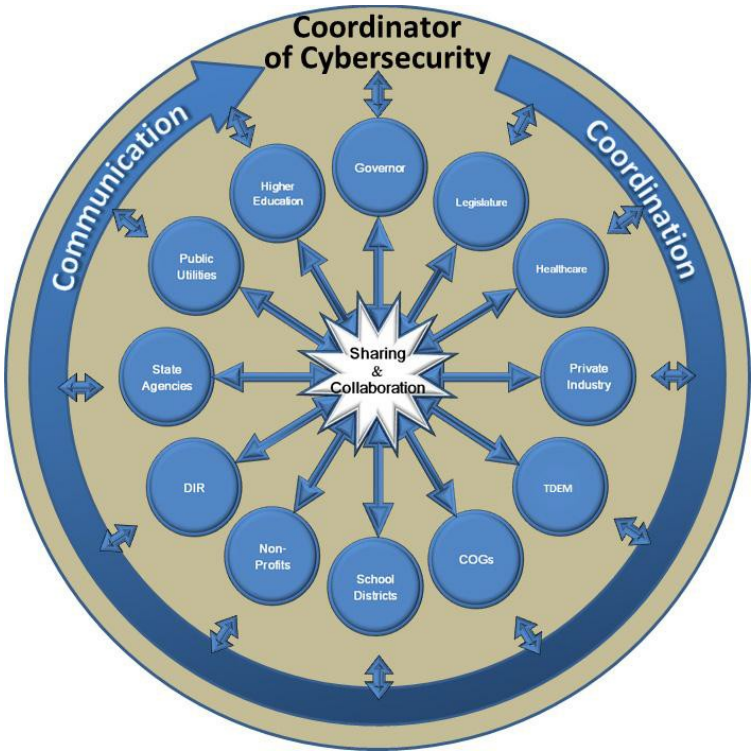


Figure 2. Coordination of Cybersecurity among Organizations

Establish the Business Executives for Texas Security (BETS) Partnership.
The challenges confronting the state's cybersecurity infrastructure are multifaceted, interrelated, and numerous. They require the collective knowledge and effort of both public and private sector entities to expedite infrastructure improvement and move the state beyond reacting to threats to an environment of more proactive prevention and protection.

For this reason, the Council recommends that the Office of the Governor, through the state Texas Coordinator of Cybersecurity, charter and facilitate a Business Executives for Texas Security (BETS) organization that unites public and private sector leaders and cybersecurity practitioners in a partnership that enables the creation of an enduring framework for knowledge sharing and collaboration, making non-proprietary and industry-recognized best practices and joint solutions more readily available for the collective improvement of cybersecurity across the state.

This group, in partnership with the state and higher education, can establish a coherent, continuing framework that will:

- Define what cybersecurity means to Texas in a succinct uniform statement of purpose.
- Provide objective feedback to the executive branch regarding proposed cybersecurity policy.
- Establish generally accepted and fundamental norms for all phases and functions of cybersecurity in Texas.
- Develop joint solutions to security problems in Texas.

- Promote government-industry partnerships and encourage participation in organizations such as the FBI-sponsored InfraGard program and other professional organizations that can help to foster government-industry relationships.
- Encourage pooling of cyber talent from industry and government with academia to facilitate collaboration between individuals and organizations with similar research interests.

Appendix D contains additional details regarding background as well as proposals for both organization and structure of the BETS Partnership.

This recommendation sets conditions for significant improvement in networking and collaboration between government and business leaders as well as cybersecurity professionals across the state toward the end of seizing the initiative and transitioning the state's cybersecurity to a more proactive posture.

Establish a "Cyber Star" program to foster improvement of cyber resiliency in both private and public infrastructure in the state as well as increasing public trust.

The program is modeled after the U.S. Department of Energy's "Energy Star" program, but would focus on the cybersecurity practices of agencies and companies rather than the energy efficiency of a product.

Participation in such a program would be voluntary and aimed at validating that the applicant:

- Maintains a program to keep its workforce educated and aware of the importance of cybersecurity.
- Uses generally accepted cybersecurity best practices and processes.
- Conforms with standards relative to cybersecurity (e.g., SANS Twenty Critical Security Controls for Effective Cyber Defense).
- Performs regular internal and external assessments of their cybersecurity program.
- Demonstrates that they use appropriate and secure technology in business processes and practices.

Figure 3 depicts how the five points of the Cyber Star, together with participation and input from public and private sector stakeholders, supports a well-rounded cybersecurity program. Appendix E discusses the general concept, key objective, and suggestions for establishing this program.

The Council believes that such a program developed and embraced by BETS with a distinct certification logo that can be displayed on an agency's or company's public website will allow potential customers to easily identify organizations with whom doing business or e-business is safe from a cybersecurity standpoint.

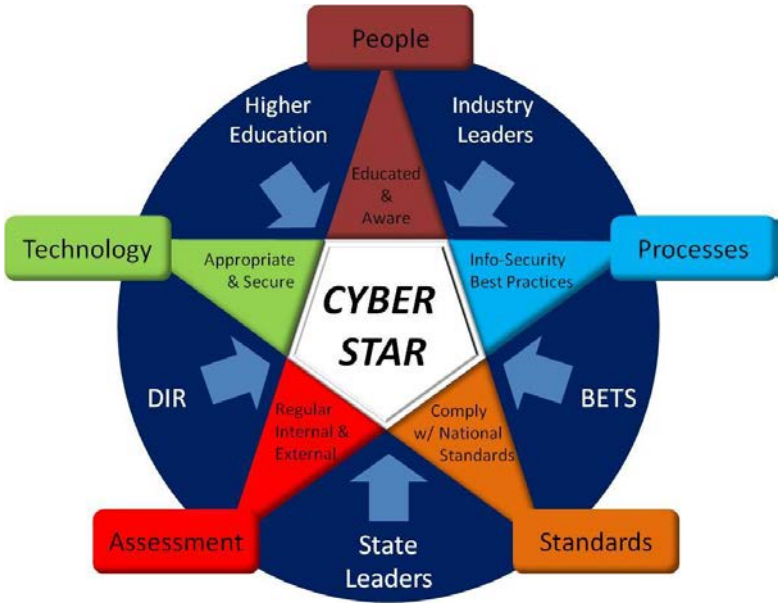


Figure 3. The Cyber Star Program

Adopt the Community Cyber Security Maturity Model (CCSMM) as a statewide guide for developing processes leading to a state of cyber maturity.

Rural communities, municipalities, and counties as well as small businesses and non-profit organizations traditionally face a tremendous task in prioritizing available resources to maintain the availability of services their constituents, customers, and clients rely on, and that must occur before consideration is given to any kind of cybersecurity program. Even well-resourced communities, governments, and organizations are often challenged in knowing where to start and what to place emphasis on when developing a comprehensive program for protecting not only the information systems and networks that connect them but also the critical infrastructures that enable these systems to function.

Developing and using maturity models is a recognized method for providing a uniform guide for establishing processes that lead to a state of maturity in an area for which the model was built. The CCSMM evolved from the need to determine the cyber preparedness of a community and to identify a prioritized plan to improve the level of preparedness. The CCSMM guides community leadership through an assessment that results in categorizing where a community fits in one of five levels of maturity:

- **Level 1 – Security Aware:** Make individuals and organizations aware of threats, problems, and issues related to cybersecurity.
- **Level 2 – Process Development:** Establish and improve on the processes required to effectively address cybersecurity issues.
- **Level 3 – Information Enabled:** Ensure that all organizations within the community are aware of the issues related to cybersecurity and have established the processes and mechanisms necessary to identify security-related events.

- **Level 4 – Tactics Developed:** Ensure that programs are designed to develop more efficient and more proactive local and strategic methods to detect and respond to attacks.
- **Level 5 – Full Security Operational Capability:** Illustrate how the top level of the model represents that the necessary processes and tools are in set in place to enable any organization to consider itself fully capable of detecting and addressing any type of cyber threat.

After determining at which level the community currently resides, the CCSMM helps leaders determine what must be accomplished in order to improve the current state of cybersecurity and better prepare to respond to cyber attacks. Appendix F contains more detailed information regarding the needs that drove the development of the Community Cyber Security Maturity Model, as well as some of the early successes resulting from its use.

Expand and strengthen DIR's Duties and Powers.
DIR's successes in recent years to develop and implement cybersecurity for state agencies must be capitalized upon and its role further developed to enable the continued growth of a comprehensive cybersecurity plan for the state's public infrastructure.

To the extent that Texas legislation currently addresses the topic of cybersecurity at all, the focus is primarily on one of reaction to a cyber crime and potential punishments (Title 7 Texas Penal Code, Chapter 33 regarding Computer Crimes) rather than any focus on prevention or protection against malicious cyber activities.

Despite best efforts, cyber crime and incidents will continue, and the need to respond remains. But just as important to the overall cybersecurity effort is identifying vulnerabilities and taking proactive measures before incidents occur. To that end, Texas Government Code sections regarding DIR's duties and powers should be reviewed and updated, and resources identified, in order to enhance DIR's efforts to lead implementation of state infrastructure improvement activities. These activities would be executed in conjunction with the Texas Coordinator of Cybersecurity and would focus on improving the state's prevention of and defense against cybersecurity incidents.

Infrastructure Summary

Advancing a cyber secure infrastructure is the foundational element for moving toward a more secure and prosperous Texas. The willingness of private industry in Texas to participate in and support focused efforts to improve cybersecurity in major metropolitan areas, as demonstrated in San Antonio, significantly raises the potential for meaningful exchange of best practices and information sharing between public and private sectors. The establishment of a Texas Coordinator of Cybersecurity in the Office of the Governor is key to seizing this opportunity and capitalizing on it for the long-term benefit of the state.

Developing the Cybersecurity Industry in the State

Findings

The Council was charged with examining specific actions to accelerate the growth of cybersecurity as an industry in the state. Regardless of the industry, the foundation for all business growth in the

state remains the same. There is no substitute for a reasonable and reliable regulatory climate, low taxes, a resilient and modern infrastructure, and a skilled workforce. Those core attributes have remained strong in Texas and are the key reasons for the state's economic strength. They are as applicable to the cybersecurity industry as they are to any other industry within the state. Since the cybersecurity industry as a whole is vital to both the state and national economy, the Council has identified five findings within industry and produced recommendations for possible solutions to those concerns:

- To grow cybersecurity investment in Texas, the industry requires access to more trained cybersecurity professionals, financial capital, and cybersecurity innovation.
- Texas must invest in cybersecurity education programs across the K–12, community college, and university levels in order to obtain the number of trained cybersecurity professionals it needs across the employment continuum.
- Texas lacks a statewide context and strategy for advancing cybersecurity industry economic development.
- There is no consistent voice for industry regarding cybersecurity policies and recommendations in the state.
- There is not enough cybersecurity collaboration, innovation, and entrepreneurship within the state.

To grow cybersecurity investment in Texas, the industry will need access to more trained cybersecurity professionals, financial capital, and cybersecurity innovation.

The Council conducted a formal survey to determine the current state of Texas' cybersecurity programs. Appendix G contains a discussion of the survey. In addition, the Council informally surveyed numerous for-profit companies, both large and small, as well as federal government agencies to include the U.S. Department of Defense (DoD). **The lack of a qualified workforce was universally cited as the single largest challenge to the productivity and growth of this industry**. In addition, individuals surveyed at the DoD and major defense contractors cited serious concerns over their difficulty in finding qualified personnel who were U.S. citizens capable of receiving the required security clearance for their work. This led to the next finding.

Texas needs to invest in cybersecurity education programs across the K–12, community college, and university levels in order to obtain the number of trained cybersecurity professionals it needs across the employment continuum.

IT professional shortages exist at three critical educational levels: certification (sub-two year degree), associate's degree (sub-baccalaureate degree), and bachelor's and post-graduate degrees. To be effective, employers, including the military and homeland security professionals, should determine the skills, knowledge and competency requirements. To address these needs, national cybersecurity skill standards were developed through a National Science Foundation Advanced Technological Education (ATE) center grant to Bellevue College in Washington State in 2003. These skill standards are aimed at the entry-level employee and are most commonly used as the basis for AAS degrees. They were recognized by the Texas Skill Standards Board and are currently available to community and technical colleges to inform curriculum alignment with employer skill needs.

However, many years have passed since those standards were developed, and the technology landscape has changed significantly during that time. As a starting point, they could provide the foundation to create new standards to meet current employer needs and provide the starting point to address curriculum development at all levels. More recently, in 2011, the National Institute of Standards and Technology (NIST) initiated the National Initiative for Cybersecurity Education (NICE) and recently published the National Cybersecurity Workforce Framework. The framework is another possible starting point to form the basis for updating Texas' cybersecurity workforce programs for high school career and technical education, community college workforce programs, and even professional education in universities.

The Council noted the work of The University of Texas at San Antonio (UTSA) and the Alamo Community College District's Information Technology and Security Academy (ITSA), as well as the support from large corporations such as USAA and Rackspace, which is well known throughout the rest of the nation and is often cited as an example of an effective focus on the issues related to cybersecurity. That reputation was earned through significant support of regional, state, and national programs developed at institutions of higher education in San Antonio. Those centers of excellence, such as The Institute for Cyber Security at UTSA, which was originally formed with funding from the Texas Emerging Technology Fund, have used state funds to leverage significant federal and other non-state funds back into UTSA and the state. Outside of San Antonio, The University of Texas at Austin's Center for Identity is another example of Texas programs leveraging non-state dollars to grow and develop their cybersecurity programs.

Texas lacks a statewide context and strategy for advancing cybersecurity industry economic development.

For a cybersecurity business to thrive in Texas, it will need access to several other key ingredients: capital, markets, technology transfer opportunities, a culture for innovation, and a healthy business climate, among others. Texas certainly has much to offer in these areas, including world-class university systems, key federal cybersecurity assets, a business-friendly climate, and a mature venture capital ecosystem. When the Governor convened the Industry Cluster Initiative in 2005, the IT cluster group discovered that federal research and development (R&D) investment in Texas over the ten-year period, 1993–2003, represents a capture of only one half of one percent—$204 million of $41 billion invested. This cyber initiative is in part about spurring innovation through R&D and capturing a greater percentage of emerging network and information technology R&D, companies and start-ups within the state. Assembling these elements into a mixture optimal for a thriving cybersecurity business climate is critical and requires considerable thought. In short, a comprehensive strategy describing a clear plan on how to accelerate growth of the cybersecurity industry in Texas does not presently exist, and the creation of such a strategy is needed at this time.

There is no consistent voice for industry regarding cybersecurity policies and recommendations in Texas.

Texas recognizes that cybersecurity influences all forms of business throughout the state, from small business to Fortune 500 companies, as well as multiple state and federal agencies inside of Texas. As

such, a formal, consistent voice for industry regarding cybersecurity polices and recommendations is needed.

There is not enough cybersecurity collaboration, innovation, and entrepreneurship within the state.

Texas could benefit from more opportunities for proactive cybersecurity collaboration and entrepreneurship. San Antonio is home to one example of this general sort of activity in the form of a unique collaborative environment known as "Geekdom." The primary goal of the program is to foster ideas and entrepreneurship in technology and to provide mentorship and assistance in a collaborative setting. Such efforts have a proven track record of "connecting the innovation dots" and increasing the entrepreneurship activity of a community.

Recommendations

Based on its understanding of the cybersecurity industry within Texas and what is needed to increase the cybersecurity industry presence within the state, the Council explored the following recommendations:

- Develop a comprehensive strategy and plan that describes how Texas will create a vibrant and robust cybersecurity industry and economy.
- Increase the number of cybersecurity professionals in the state.
- Provide a consistent voice for industry regarding cybersecurity policies.
- Continue investing in higher education cybersecurity programs.
- Promote collaboration, innovation, and entrepreneurship in cybersecurity.

Develop a comprehensive strategy and plan that describes how Texas will create a vibrant and robust cybersecurity industry and economy in the state.

The state must have an understanding of what is needed to create an environment that is enticing to the cybersecurity industry. The goal is to use this understanding to establish a strategy and direction which will help to create this environment to promote cybersecurity industry within the state. Consideration must be given to the way Texas cybersecurity businesses will gain access to people, capital, markets, technology transfer opportunities, a culture of innovation and entrepreneurship, and other factors that will lead to the growth of the industry. Discussions with leaders from other states that have made cybersecurity a statewide priority, such as Maryland, will be valuable in incorporating best practices.

Finally, the industry and economic growth strategy that must be created must ensure proper coordination with critical infrastructure considerations so that the right balance of economic growth and infrastructure development is met. During the 1980s, SEMATECH was formed in Austin to support the national security needs of the nation by acting as a hub for shared research and development in the non-competitive domain of semiconductor manufacturing. Today, a similar opportunity exists to form an organization focused on computer, software, network, and human systems related to cybersecurity.

Increase the number of cybersecurity practitioners in Texas.
Through the information gathering by Council, it was revealed that Texas lacks the number of cybersecurity professionals it needs to both secure its own assets as well as to encourage additional industry to locate within the state. Texas must increase its number of cybersecurity professionals for both the cybersecurity industry and industry in general.

Increasing the number of cybersecurity practitioners is important, but it can't be done without developing an understanding of the skills needed by our business community. There are many aspects to cybersecurity often requiring unique skill sets. In cooperation with our industry partners, the state must determine what specific cybersecurity skills are needed and establish a method to address this need. The BETS organization should work to identify skills, knowledge, and competencies required for entry-level positions and then work with the Texas Higher Education Coordinating Board (THECB) and the Texas Skills Standards Board to revise and update standards for degrees based on the competencies identified.

Many factors affect the number of individuals who desire to pursue an education in cybersecurity-related disciplines. Increasing the number of cybersecurity practitioners requires more than just addressing the curriculum issues. Addressing issues directly impacting students must also be considered, including:

- Instituting post-secondary loan forgiveness for critical cybersecurity degrees.
- Initiating an aggressive campaign to inform students, parents, and educators of the supply and demand gap, along with real time data on wages to incent behavioral change at the educational front end.
- Identifying barriers at institutions of higher education to eliminate attrition rates within IT degree plan.
- Encouraging four-year institutions of higher education to work closely with two-year institutions to establish articulation agreements enabling students to advance their cybersecurity educational opportunities.

Provide a consistent voice for industry regarding cybersecurity policies.
Texas must address the need for a representative and consistent voice for industry regarding cybersecurity policies and recommendations. This entity can facilitate communication in both directions—from the state to industry and from industry to the state. The industry and economic growth strategy that must be created needs to ensure proper coordination with critical infrastructure considerations so that the right balance of economic growth and infrastructure development is met. This entity can go a long way toward establishing a single entity within the state to provide a consistent voice on cybersecurity issues for industry. This entity, whether BETS specifically or another advisory group formed in response to this recommendation, should:

- Provide policy development assistance to DIR and the Texas State Legislature.
- Be appointed by the Governor and have legislative authority to form additional committees, invite members, and form additional support groups.
- Meet at least annually to provide recommendations to DIR's Executive Director or at the request of the Governor or the Legislature.
- Receive support funding from the state or through the Texas Economic Development Corporation (Texas One).

Continue investing in higher education cybersecurity programs.
An earlier recommendation addressed the need to develop curricula as well as programs to attract students to the cybersecurity field. The state must also recognize the importance of higher education to the cybersecurity efforts and encourage continued support of programs at this level. This can be accomplished through a number of initiatives including:

- Recognizing the benefit of higher education infrastructure development in cybersecurity by continuing to fund efforts at established centers of excellence, as well as developing new programs in cooperation with existing centers throughout the state.
- Funding for the centers of excellence and new programs through the regular biannual legislative progress or through existing state programs such as the Texas Emerging Technology program.
- Facilitating private industry cooperation through incentives in the funding of additional centers of excellence and requiring centers within the state to foster collaboration opportunities.
- Encouraging institutions of higher education to become Community Centers of Excellence in Cybersecurity to help their own communities establish and maintain viable and sustainable cybersecurity programs.

Promote collaboration, innovation, and entrepreneurship in cybersecurity.
Texas should highlight the benefits of collaborative efforts between education and industry and encourage the development of new businesses with innovative ideas in cybersecurity. Initiatives in this regard would include:

- Texas encouraging the continued development of collaborative entrepreneurship program, such as "Geekdom," throughout the state.
- Texas Institutions of Higher Education working directly with industry and non-profit organizations to develop collaborative entrepreneurship programs in their areas.
- Texas providing additional funding through university participation or through specific legislative appropriation.
- Utilizing existing organizations such as the alumni networks found in the UT and Texas A&M systems to encourage entrepreneurs and establish partnerships.

Industry Summary

As illustrated in the recommendations in this section, economic development cannot be accomplished without establishing a culture of cybersecurity within Texas. Cybersecurity does not exist solely in any one sector but is found across the spectrum of government, academia, and industry. The Council's chief findings and recommendations in this area highlight the need for better

coordination between the state and industry and reiterate the importance of the development of an entity such as BETS while also identifying the need for more cybersecurity practitioners. The next section speaks to the creation of the overarching need for the establishment of a cybersecurity culture within the state.

Creating an Enduring Cybersecurity Culture

Findings

There were two key Council findings regarding cybersecurity education in Texas. First, the education and professional training institutions in Texas are not producing enough qualified cybersecurity professionals to meet the needs of employers in Texas. A poll conducted by this Council of key business leaders in Texas indicates a shortage of a qualified cybersecurity workforce in Texas. A similar finding at the national level is reflected in a November 2010 federal report from the Center for Strategic & International Studies (CSIS), titled "A Human Capital Crisis in Cybersecurity." Secondly, the Council found that Texas lacks a coordinated and developed cybersecurity awareness program for Texans.

Recommendations

Both findings can be addressed by creating an enhanced and coordinated cybersecurity education program in Texas. The term "education," as used in this report, includes education as delivered through institutions of learning, professional training, and awareness training. The audience for cybersecurity education can be generally categorized as "cybersecurity practitioners" and "all other Texans." The term "practitioners" includes both cybersecurity professionals and information technology professionals. Cybersecurity education for practitioners must lead to positive job placements in the current and future marketplace.

Accordingly, the education curricula would be different for these two groups. The types of education programs that would be focused for cybersecurity practitioners should include the following:

- Masters, PhD, and post-doctoral formalized educational programs that include both education and research components.
- Four-year degrees focusing on cybersecurity areas—generally in computer science, information systems, computer engineering, cybersecurity, information assurance, or related fields.
- Two-year associate degrees, diplomas, or certificates in information systems, cybersecurity, information assurance, or related fields.
- Industry and educational institution-delivered cybersecurity-related professional training that prepares students for cybersecurity-industry recognized certifications.

For all other Texans, a general cybersecurity awareness curriculum should be developed. Cybersecurity awareness programs should be ongoing, and the curriculum contents should be current, relevant, succinct, and easily available.

A number of good strategies have been outlined at a national level to address the cybersecurity workforce development and to improve other aspects of cybersecurity education. This report does not plan to duplicate those strategies but instead provides some actionable recommendations.

However, there may be opportunities to leverage some of the national strategies as part of implementing certain recommendations made in this report.

BETS should include a senior representative from THECB and from the Texas Education Agency (TEA). Subsequent working groups could leverage expertise from the education community and other agencies as appropriate.

As a first step, BETS should set in motion activities to create the Texas Cybersecurity Education Pipeline (see Figure 4 below). A major activity toward building a successful Cybersecurity Education Pipeline is to enhance and coordinate existing science, technology, engineering, and mathematics (STEM) programs as well as computer science and IT elective programs in schools as these programs form the general basic pool from which cybersecurity studies, and subsequently cybersecurity graduates, can be developed.

BETS, working with appropriate partners, should also explore options to introduce new cybersecurity education curriculum in junior high and high schools, actively promote dual credit programs in high schools in the cybersecurity field (similar to the Information Technology and Security Academy, one of the Alamo Academies in San Antonio), develop robust regional Programs of Study (also known as "career pathways") with local independent school districts, community colleges, and universities, encourage professional mentorship of students, and establish community college and higher education collaborations for those seeking advanced cybersecurity degrees. Formalized cybersecurity education curricula should also produce graduates who are prepared to earn industry-recognized professional IT certifications such as A+, Network +, Security +, CCNA, CISSP, CISM, GIAC, etc.

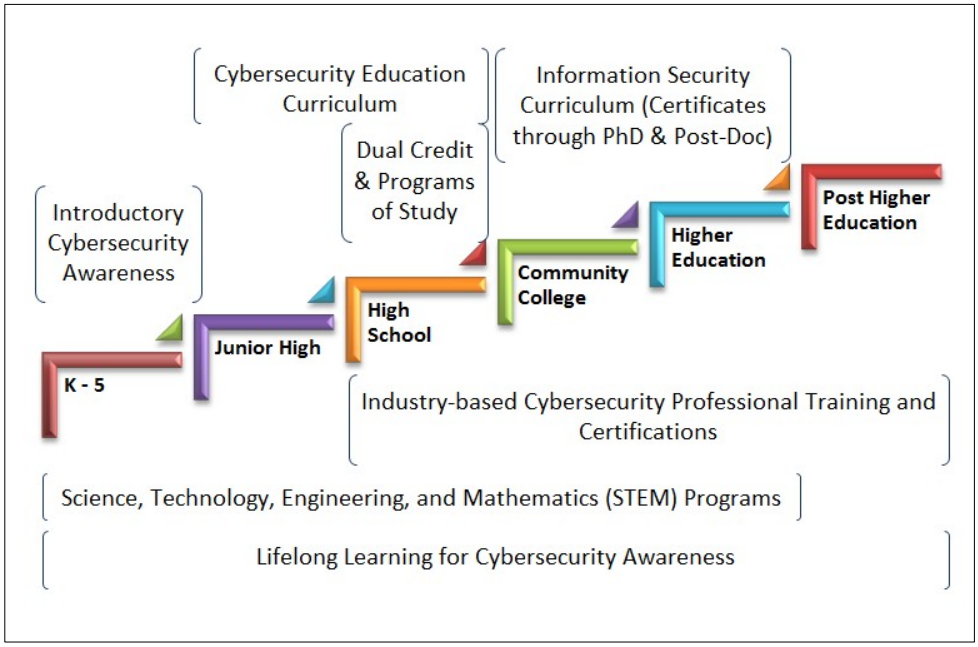


Figure 4. Proposed Texas Cybersecurity Education Pipeline

In addition to exploring new and innovative ideas and partnerships to promote the Cybersecurity Education Pipeline, BETS can also help to facilitate the coordination and growth of existing innovative programs such as the CyberPatriot high school cyber defense competition, the National Collegiate Cyber Defense Competition, the Cyber Quest Challenges for college students and adults, and the DoD DC3 Digital Challenge by inviting high schools and colleges across Texas to join in and encourage communities to support them with volunteer mentors, instructional clinics, recognition programs, and grants.

The promotion of these programs could lead to the creation of a Texas Digital Challenge with state-level recognition and eventually to national participation in cybersecurity competitions such as the National Collegiate Cyber Defense Competition and the International Capture the Flag event.

BETS can also foster partnerships between education and industry that would lead to internship programs that help develop skilled graduates in cybersecurity fields, mentorship programs, and collaborative research and establish employee training programs in cybersecurity areas.

To provide an incentive to enter the Texas Cybersecurity Education Pipeline, the BETS group might explore creation of a Texas version of the federal Scholarship for Service (SFS) program which provides tuition and support for individuals in cybersecurity-related programs. Alternatively, or additionally, a loan forgiveness program for students should also be explored.

To increase cybersecurity awareness in Texas, the Council recommends that DIR's role be reviewed and sharpened so that DIR can take a leadership role in establishing a sustainable Cybersecurity Awareness Program for all Texans. Not only are national security and economic data at risk, the personal safety and wealth of individual Texans are also at risk, unless Texans' general cybersecurity awareness is enhanced sufficiently to protect them from increasingly sophisticated social engineering and other cybersecurity exploits. DIR should be provided appropriate resources and authority and should work with the Texas Coordinator of Cybersecurity (proposed in the Infrastructure section). Where feasible, DIR could also leverage work already done by other agencies such as the Texas Attorney General's Identity Protection initiative and other established cybersecurity awareness programs in state agencies and higher education. These education and awareness efforts should include programs targeted toward legislators and key stakeholders at all levels of government that are in a position to influence cybersecurity awareness program adoption for their constituencies.

Education Summary

The Council repeatedly noted the need for a trained workforce as it studied cybersecurity issues in Texas. While Texas has much going for it, such as the number of university centers of excellence in cybersecurity, much more must still be accomplished. This is especially true when education is viewed more broadly, as it must be in cybersecurity, and extends beyond formal degree-granting programs to include the Texas citizens who are responsible for securing their own systems and networks.

The ultimate goals of cybersecurity education in Texas would be to provide a well-trained workforce of cybersecurity practitioners steeped in a “Culture of Security” and to create a “Culture of Security Awareness” among all Texans.

Next Steps

During the 1980s, SEMATECH was formed in Austin to support the national security needs of the nation by acting as a hub for shared research and development in the non-competitive domain of semiconductor manufacturing. Today, a similar opportunity exists to form an organization focused on computer, software, network, and human systems related to cybersecurity.

The Council believes that it is important that Texas takes some immediate steps in order to address the issues raised in this report. The first step, which can be accomplished in the first half of 2013 is:

- Through Executive Order, establish a "Business Executives for Texas Security" (BETS) partnership.

This recommendation can be completed without the need for additional funding or legislative approval. It can be accomplished by the Office of the Governor and would not only demonstrate Texas' commitment to enhancing cybersecurity in the state but also would set the stage for addressing additional recommendations. While BETS can be established in the first half of the year, it will take additional time to select the membership and begin discussions. The goal should be to have a first meeting in the second half of 2013.

During the 83rd Texas legislature, additional steps can be taken to implement the recommendations made by the Council. These next steps will require legislative action and include:

- Establishing a Texas Coordinator of Cybersecurity within the Office of the Governor.
- Empowering DIR to lead implementation of state infrastructure improvement activities in coordination with the Texas Coordinator of Cybersecurity.
- Funding implementation of a program to institute the Community Cyber Security Maturity Model in communities throughout Texas.

Accomplishing these steps in 2013 will provide the leadership necessary to advance Texas' cybersecurity agenda. Once the Texas Coordinator of Cybersecurity within the Office of the Governor is selected, the individual should quickly meet with BETS in order to continue and advance efforts through 2014 and beyond. At that point, additional steps can be taken to advance the cybersecurity agenda in the state including:

- Utilizing BETS to define a roadmap to improve cybersecurity for key critical infrastructure and industry in the state and increase additional cyber technology investment sources.
- Under DIR leadership, developing a sustainable cybersecurity awareness program for all Texans.

When discussing cybersecurity and industry, the Council noted that BETS must address two issues. The first is the growth of the cybersecurity industry within the state. Cities such as San Antonio have a robust cybersecurity industry which other technology corridors within the state could follow. The second aspect that cybersecurity and industry need to be examined from is "cybersecurity within industry." This differs from the first in that all industries, regardless of focus, must be concerned with cybersecurity. Cultivating a culture of security within communities and throughout Texas in

which all individuals and organizations are concerned with cybersecurity will help to advance the state's overall posture of cybersecurity. The Council believes that this in itself could become a marketable commodity that could be used not only to attract additional cybersecurity industry to Texas but could also result in an overall increased attraction of industry in general to Texas. The idea is to build on the premise that the strong cybersecurity culture in Texas is such that cyber incidents would be less likely to occur; when they do occur, it is more likely that a coordinated response to the incident will take place, resulting in lower impact to the affected organization.

Following these steps in 2014 will allow the appropriate organizations to address all of the recommendations in this report without a need for the Council to continue as currently tasked. However, as cybersecurity is an ever-changing issue, the Council believes that it might be useful to form another council with a similar charter in 2015 to report on the state's progress and to make necessary adjustments based on either technological or economic factors that may have changed.

Conclusion

There is no question that every day millions of people entrust entities within the State of Texas with personal, financial, and other sensitive information requiring protection at the highest levels. Millions more rely on critical infrastructure networks within the state for basic life needs such as power, water, emergency response, and others. However, as society's reliance on technology continues to increase, so do the ramifications of successful attacks on our technology infrastructures. Sadly, the daily news headlines are full of information security breaches and other results of cyber malfeasance throughout the world.

The good news for Texas is that, through the information gathering conducted during the course of working on this report, the Council found that Texas already has strengths across a spectrum of areas critical to successful cybersecurity efforts. From legislative mandates requiring state agencies to implement basic levels of cybersecurity (such as those found in Texas Administrative Code 202), to multiple Centers of Academic Excellence in Information Assurance, to successful models of metro-area participation in cybersecurity programs and innovation centers, these strengths encompass multiple levels of Texas government, geographic diversity, and public/private collaborations.

What the Council found missing is the framework necessary to collaboratively tie these cybersecurity strengths together. Texas is not alone in this regard. States throughout the nation are struggling to identify successful strategies for addressing cybersecurity concerns.

In crafting the recommendations contained in this report, the Council worked diligently to address the state's challenges while building on its strengths and adhering to the legislative mandate to utilize existing resources. The resulting framework recommendations are both innovative in their approach and straightforward in their purpose. The success of framework implementation will depend on the commitment of the stakeholders in making cybersecurity a priority initiative for Texas. This is especially true in light of recognizing that failure to act on the cybersecurity threat now could adversely impact other key focus areas, such as energy security and border security, for the state.

The benefits of implementing a framework such as recommended in this report extend beyond cybersecurity concerns, and have the ability to improve the well-being of the state in a variety of ways. Increased economic development as a result of these efforts is, of course, a key benefit affecting all Texas citizens. However, it is not the only one. For example, one of the key challenges the Council faced in our information gathering was the act of distributing the public sector survey. While many organizations were identified to participate, efforts to communicate with the organizations proved to be difficult. The establishment of formal communication and collaboration channels among diverse Texas organizations (including municipalities, public and private organizations, and educational institutions) can serve to identify and enhance a wide-range of initiatives throughout Texas.

To be clear, Texas is in a unique position not only to implement a gold-standard level of protection of the state's information assets, but also to become a nationwide leader in cybersecurity that other states can emulate. It is the Council's intention that the recommendations provided in this report will provide the necessary roadmap for the state to achieve the goals of "Building a Secure and More Prosperous Texas." With an increasingly advanced and multi-dimensional threat growing in cyberspace, failure to take comprehensive action now puts all Texas institutions and citizens at significant risk.

Now is the time for Texas to lead. ✯

Acknowledgements

The Council would like to thank the following individuals and organizations for their assistance in the creation of this report:

- Dr. John Frederick, Provost, The University of Texas at San Antonio
- Bobby R. Inman, Admiral, U. S. Navy, (Ret.)
- Mark Weatherford, Deputy Under Secretary, U.S. Department of Homeland Security

- AT&T
- CSIdentity (CSID)
- James A. Baker III Institute for Public Policy, Rice University
- Federal Bureau of Investigation
- Gartner, Inc.
- The Greater San Antonio Chamber of Commerce
- National Security Agency
- National White Collar Crime Center
- Texas Army National Guard
- Texas Statewide Information Security Advisory Committee (SISAC)
- USAA
- Valero

In addition to those listed above, through our information gathering efforts the Council received information and feedback from a multitude of organizations and citizens throughout Texas. This information was invaluable in the formulation of our recommendations and this report, and we recognize the contributions of all who assisted us in these efforts. The Council also thanks Vivian Cullipher, Publications Specialist at the Texas Department of Information Resources, for her editing and production contributions.

Appendix A

SB 988 Tasking

The Texas Cybersecurity, Education, and Economic Development Council was created by Senate Bill 988, included below:

A BILL TO BE ENTITLED
AN ACT

relating to the creation of a cybersecurity, education, and economic development council.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. Chapter 2054, Government Code, is amended by adding Subchapter N to read as follows:

SUBCHAPTER N. CYBERSECURITY, EDUCATION, AND ECONOMIC DEVELOPMENT COUNCIL

Sec. 2054.501. DEFINITION. In this subchapter, "council" means the Cybersecurity, Education, and Economic Development Council.

Sec. 2054.502. CYBERSECURITY, EDUCATION, AND ECONOMIC DEVELOPMENT COUNCIL; COMPOSITION. (a) The Cybersecurity, Education, and Economic Development Council is established.

(b) The council is composed of nine members appointed by the executive director. The members must include:

(1) one representative from the department;

(2) one representative from the Texas Economic Development and Tourism Office in the office of the governor;

(3) two representatives from institutions of higher education with cybersecurity-related programs;

(4) one representative from a public junior college, as defined by Section 61.003, Education Code, with a cybersecurity-related program;

(5) one state military forces liaison experienced in the cybersecurity field; and

(6) three representatives from chamber of commerce organizations or businesses who have a cybersecurity background.

(c) The council shall elect a presiding officer from among its members.

(d) A council member serves at the pleasure of the executive director.

Sec. 2054.503. COMPENSATION. A council member serves without compensation or reimbursement of expenses.

Sec. 2054.504. COUNCIL POWERS AND DUTIES. (a) The council shall:

(1) at least quarterly, meet at the call of the presiding officer; and

(2) conduct an interim study and make recommendations to the executive director regarding:

(A) improving the infrastructure of this state's cybersecurity operations with existing resources and through partnerships between government, business, and institutions of higher education; and

(B) examining specific actions to accelerate the growth of cybersecurity as an industry in this state.

(b) The council may request the assistance of state agencies, departments, or offices to carry out its duties.

Sec. 2054.505. REPORT. Not later than December 1, 2012, the council shall submit a report based on its findings to:

(1) the executive director;

(2) the governor;

(3) the lieutenant governor;
(4) the speaker of the house of representatives;
(5) the higher education committees of the senate and house of representatives;
(6) the Senate Committee on Economic Development;
(7) the House Technology Committee; and
(8) the House Economic and Small Business Development Committee.

Sec. 2054.506. EXPIRATION OF SUBCHAPTER. This subchapter expires and the council is abolished September 1, 2013.

SECTION 2. Not later than the 30th day after the effective date of this Act, the executive director of the Department of Information Resources shall appoint the members of the Cybersecurity, Education, and Economic Development Council as established by Subchapter N, Chapter 2054, Government Code, as added by this Act.

SECTION 3. This Act takes effect September 1, 2011.

Appendix B

Council Membership

Council Members	
Robert Butler, Chair	Chief Security Officer/Senior Vice President, IO
Dr. Gregory White, Vice-Chair	Director, Center for Infrastructure Assurance and Security, The University of Texas at San Antonio
Dr. David A. Abarca, CISSP	Asst. Professor and Information Security Program Director, Del Mar College
Dr. Frederick Chang	President and Chief Operating Officer, 21CT, Inc.
Angel Cruz 12/2011–current (replaced Todd Kimbriel)	Chief Information Security Officer, Department of Information Resources
Mary Dickerson, CISSP	Executive Director of IT Security and Chief Information Security Officer, University of Houston/University of Houston System
B. Keith Graf 09/2012–current (replaced Jonathan Taylor)	Director, Aerospace, Aviation, and Defense, & Texas Military Preparedness
Todd Kimbriel 10/2011–12/2011	Director of E-Government, Department of Information Resources (DIR)
Sam Segran, GIAC-GSLC	Chief Information Officer, Texas Tech University
Col. Timothy M. Smith, CISSP	Chief Information Officer, Texas Army National Guard
Jonathan Taylor 10/2011–09/2012	Director, Texas Emerging Technology Fund

Ex Officio Council Members	
Karen Robinson	State of Texas Chief Information Officer Executive Director, Texas Department of Information Resources
Carl Marsh	Chief Operations Officer, Texas Department of Information Resources
Lori Person	Chief Administrative Officer, Texas Department of Information Resources
Martin Zelinsky	General Counsel, Texas Department of Information Resources
Chandra Thompson	Secretariat, Texas Department of Information Resources

Appendix C

Glossary

In the report, a number of terms were used which may have a different meaning to individuals with different backgrounds. For the purpose of this report, the following terms and how they are used in the report are as follows:

Botnet: Derived from the terms “robot” and “network,” a botnet is a network of private computers that are infected with malicious software and controlled as a group by a malicious person or party. Computers are infected without the computer owner's awareness to automatically send out "Spam" email messages, spread viruses, attack computers and servers, and commit other kinds of cybercrime and fraud.

Credentials: A type of identity data used in a computer system to confirm the identity and authenticate the approved level of access of a given user; most often associated with User ID and Password, but may also use SmartCard and PIN, biometrics, or a set of personal questions that the user must answer.

COGs: Councils of Government

Cyber: Of, relating to, or involving computers or computer networks.

Cyber-attack: A cyber-attack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber-attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.

CyberPatriot: A high school cyber defense competition run by the Air Force Association which encourages high school students to learn more about cybersecurity through a hands-on competition environment. More can be learned about the program by visiting the CyberPatriot website at www.cyberpatriot.org.

Cyber Quest Challenges: The challenges are a series of on-line competitions which have been designed to challenge participants in a variety of different information security related tests. More information can be found on the challenges at http://uscc.cyberquests.org.

Cybersecurity: Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack; also the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

Cybersecurity as an industry: means any business entity that creates and markets security products and services and can also include any company with significant cybersecurity requirements or needs based on their business functions or processes.

Cybersecurity business: Public and private companies who create and market security products and services, and technology companies with significant cybersecurity process capabilities.

Cybersecurity infrastructure: The data centers, networks, servers, computing and telecommunications devices, end users, and controls that protect and support electricity generation, transmission and distribution; gas production, transport and distribution; oil and oil products production, transport and distribution; telecommunication; water supply (drinking water, waste water/sewage, surface water); agriculture, food production and distribution; heating (e.g. natural gas, fuel oil, district heating); public health (hospitals, ambulances); transportation systems (fuel supply, railways, airports, harbors, inland shipping); financial services (banking, clearing); security services (police, military).

Cybersecurity operations: means administrative and technical measures taken to protect the state against unauthorized access or attack, including preventing against criminal or unauthorized use of electronic data.

Data breach: The intentional or unintentional release of secure information to an untrusted environment.

DC3 Forensics Challenge: A cybersecurity competition focusing on digital forensics sponsored by the DoD Cyber Crime Center. The competition is open to individuals or teams from high school through post-higher education levels.

InfraGard: InfraGard (www.infragard.net) is a partnership between the Federal Bureau of Investigation and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.

ISP: Internet Service Provider. Any one of many organizations that are community-owned, non-profit, privately owned, or for-profit and provide access to the Internet.

Malware: Short for "*mal*icious soft*ware*." Refers to a variety of hostile or intrusive software created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems (i.e., viruses, worms, Trojan horses, spyware, adware, etc.).

NCCDC: The National Collegiate Cyber Defense Competition (NCCDC) is the largest collegiate cyber defense competition. It consists of several rounds of competition throughout the nation leading to the national championship held in San Antonio every year. It is only open to college teams though both 2-year and 4-year institutions may participate and even allows a small number of graduate students per team. More information can be found at their website at www.nationalccdc.org.

Phishing: The act of attempting to acquire private information, such as user names, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication; an example of social engineering techniques used to deceive users and exploit the poor usability of current web security technologies.

TDEM: Texas Division of Emergency Management (previously "GDEM," or "Governor's Division of Emergency Management"). Operated within the Texas Department of Public Safety, TDEM implements programs to increase public awareness about threats and hazards, coordinates emergency planning, provides an extensive array of specialized training for emergency responders and local officials, and administers disaster recovery and hazard mitigation programs in the State of Texas. See www.txdps.state.tx.us/dem/about.htm for more information.

Appendix D

Business Executives for Texas Security (BETS) Concept

Background and Purpose

- Texas critical infrastructure and security are at increasing risk to both physical and cyber threats. The commercial technology market and the exploitation of this market by nations, terrorists and criminal groups are evolving in ways that present serious risk to the security of Texas infrastructure and Texans. A closer dialogue with Texas industry leaders is needed to create an enabling and enduring framework for addressing today's security risks to Texas and creating a forum for continued engagement in today's technology marketplace.
- The Texas Legislature, in conjunction with the Office of the Governor, has recognized this risk and passed Senate Bill 988 in 2011, establishing a new Texas Cybersecurity, Education and Economic Development Council (Council) to address this risk.
- Recognizing the need for all of Texas' leaders to come together to address this risk, the Council strongly recommends the formation of a new public-private sector partnership, led by the Office of the Governor, with participation from key Executive branch members, key legislators and Texas "industry captains."

Organization and Structure

The Council proposes the following organization and structure for the new Business Executives for Texas Security (BETS) partnership.

- The Texas Legislature shall ensure statute is in place to support the stand-up of BETS, enabling liability protection for company leaders that are selected to participate and government guidance to prevent unfair business practices and full participation by Government members.
- The Governor shall establish an Executive Steering Group (ESG) of key Government leaders and private sector leaders in Texas as the core of the BETS partnership.
    - Government leaders will include, but are not limited to the Lieutenant Governor, Speaker of the House, Attorney General, Chief Information Officer, and Legislature Chairs of related oversight committees, including those pertaining to science, technology, and economic development.
    - Private sector leaders will include no less than six and no more than ten CEOs from Texas critical infrastructure companies to include telecommunications, information technology, energy, transportation and financial services. The Office of the Governor, in conjunction with BETS Legislative leads, may select industry leads.
    - Leaders from other Texas non-profit organizations will include no less than two and no more than four members.

- The BETS partnership should include a senior representative from the Higher Education Coordinating Board (THECB) and from the Texas Education Agency (TEA). Subsequent working groups could leverage expertise from the Education community and other agencies as appropriate.
- The Governor shall select an industry co-chair who can help the Office of the Governor set the agenda for the BETS partnership.
- The BETS partnership will also have an Operations Working Group, co-chaired by a member of the Office of the Governor and an industry co-chair at the SVP level. The Operations Working Group, under the guidance of the ESG, shall be the BETS arm responsible for executing the ESG agenda, convening Subject Matter Experts and "solutioning" to improve Texas' security posture in the state.
- The BETS partnership, at the ESG level, shall meet at least twice a year and can meet more frequently at the direction of the Office of the Governor and the industry co-chair. The Operations Working Group shall meet as frequently as required to execute the ESG agenda.

Appendix E

Cyber Star Program

General Concept

Similar to the U.S. Environmental Protection Agency's ENERGY STAR program, a Texas Cyber Star program is envisioned as a joint program developed and championed by both public and private sectors (ideally by Business Executives for Texas Security or BETS) to encourage voluntary participation by public and private organizations and aimed at validating that applicants:

- Have a program to keep its workforce educated and aware of the importance of cybersecurity
- Use generally accepted cybersecurity best practices and processes
- Conform with national standards relative to cybersecurity
- Perform regular internal and external assessments of their cybersecurity program
- Demonstrate that they use appropriate and secure technology in their business and/or processes

Objective

The intent of this program is to increase general cybersecurity confidence, both on the part of the public and private organizations who chose to participate in an effort to improve their own e-business environments, as well as among the members of the general public who are customers and clients of those organizations.

Key Suggestions

- Give the private sector the lead in developing this program, including establishing participation criteria, in partnership with the public sector through the BETS organization.
- Limit DIR's role in establishing and promulgating standards or certification requirements for the program to no more than that of any other BETS participant.
- It may be worth considering a model where companies could self-certify either by conducting their own internal audits or contracting with a third party.
- Give consideration to possible incentives (i.e., public/private prize regime) in which Texas-based companies sponsor prizes based on exceptional performers in various categories.
- Leave BETS as much implementation leeway as possible to make the program inviting to the private sector.
- Develop a distinctive certification logo that participants can display.

Appendix F

Community Cyber Security Maturity Model

Excerpted from "A Grassroots Cyber Security Program to Protect the Nation" by Gregory B. White, Ph.D., in the Proceedings of the 45th Hawaii International Conference on System Sciences – 2012

1. Introduction

Many lessons were learned from responding to the attacks of September 11, 2001. This was an event that affected the nation and ultimately had a global impact. While the U.S. federal government was attempting to deal with the impact of the attacks, one lesson that was being learned was that while the event was an attack on the nation, it was the local first responders that had to deal with the immediate effects of the attack. Since that time the nation has spent a considerable amount of money improving the ability of local and state governments and their first responders to deal with an attack of this nature. The lessons that have been learned by the first responder community are equally applicable to the cyber security community. A critical lesson to learn is that while there are numerous cyber events that might have a national level impact, they will also have an impact on state and local entities and local government leaders and cyber first responders need to be prepared to address cyber events that may occur which will have a negative impact on the community.

This paper examines several cyber incidents that have occurred at the local and state levels that illustrate how communities are increasingly becoming reliant upon the various cyber infrastructures and how a cyber event can have a negative impact on the community. This leads to the obvious conclusion that something must be done and the paper introduces a model to help communities develop viable and sustainable cyber security programs. The implementation of this model is discussed and results based on feedback from state and local officials are presented.

2. Threats to Communities

There are many benefits and reasons for introducing electronic-government at the local level. Governments see increased access, convenience, customer support, lower costs, and more access to information as reasons to increasingly rely on computer systems and networks to provide services to their citizens. [1] While all of these are benefits, the increased reliance on networks, and in particular the Internet, introduces a potential weakness as any of a variety of cyber security events can impact the delivery of the services. There are numerous examples of government entities at various levels experiencing a problem.

In February, 2009 a virus infected almost 500 of the city of Houston's computer systems. [2] The infection caused the city to shut down part of its municipal courts system including suspending arrests for minor offenses. In addition, the Houston Emergency Center was forced to disconnect from the city network for several hours and forced 3000 people to have their court appearances rescheduled. [3]

While it could be argued that the impact of this incident was minimal – only affecting 3000 citizens already in the system plus

allowing a small number of individuals who had committed minor infractions to avoid arrest – other incidents had considerably greater impact. In April, 2009, a fiber optic cable was deliberately cut in several locations in Silicon Valley. This resulted in loss of 911 access for thousands of customers. [4] In addition, tens of thousands of citizens found they had lost Internet access as well as landline and wireless phone service. [5] The loss of 911 service is obviously critical to a community. An example of another potentially significant issue is the security of electronic voting systems. There has been quite a few studies on this subject, including one event in 2010 in which the Washington D.C. election board invited groups or individuals to attempt to break into the city's voting system. One group was soon successful in gaining sufficient control to be able to both view and change votes. [6] While this was a public test, it is easy to imagine the potential implications had this flaw not been exposed at that time.

Other incidents illustrate additional events that threaten governments at various levels. In May, 2011, MSNBC posted a story regarding a security researcher penetrating the computer inside a police cruiser. The level of access obtained allowed the researcher to compromise telnet and ftp services as well as to view the current feed from the car's camera and its stored videos. [7] In another well publicized incident, the state of Virginia was the target of an extortion attempt by an attacker who claimed to have broken into a patient database and then encrypted millions of records maintained by the Virginia health agency. [8] The attacker, who also claimed to have deleted the original file, demanded a $10 million ransom for the password that would decrypt the file. Since every state and community will likely have multiple files or databases with sensitive information about its citizens, this incident illustrates the potential harm that might occur should sufficient security not be provided. It also shows that there are individuals that are willing to target states and communities and to attempt to extort money from them.

The types of issues seen in these examples are not confined to the United States. In July, 2010, the website of the Mumbai Cyber Crime Cell was hacked, embarrassing the cyber crime department of the city's law enforcement agency. [10] The group claiming responsibility for the hack also claimed to have "tampered with the information about most wanted criminals, which included some suspected terrorists." [10] In another incident in Queensland Australia, a disgruntled individual attacked the computer control systems that managed the city's wastewater. He was able on numerous occasions to divert the flow so that as much as 1 million liters of raw sewage was dumped onto the grounds of parks, waterways, and a local tourist resort. [11] All of these example serve to show how the various cyber systems, networks used in the daily operation of the various critical infrastructures in a community, can be attacked and cause mild to severe disruptions in the community. In order to address this, communities need to establish their own cyber security programs and cyber incident handling processes and procedures. Unfortunately, very few communities have such programs and in fact few even have an idea of where to begin.

3. Initial Efforts to Establish Programs

After the physical attacks that occurred September 11, 2001, many state and local governments placed an increased emphasis

on preparing to deal with terrorist attacks using any of the traditional weapons of mass destruction. No real effort, however, was placed on cyber security at the local level. At the national level, discussions were widely held regarding the possibility of a cyber terrorist attack. Efforts were under way at various federal agencies to determine ways to secure the national cyber infrastructures. These efforts were focused on cyber events that would impact the entire nation (or a major portion of it) and involved discussions on how the various federal agencies would interact with industry to address the incident and work toward a resolution. Industry was recognized as a key component of a national response because the majority of the Internet was under the control of industry and not the government. State governments were only minimally considered – basically through the establishment of the Multi-State Information Sharing and Analysis Center (MS-ISAC). No efforts were undertaken to help prepare local governments to address a cyber incident. The problem with this was twofold. First, as has been discussed, should a national cyber event occur, just like the events of 9/11, it is a national incident but state and local officials will be impacted and will need to be able to handle their response to it. Second, a national strategy that doesn't include a state and local piece completely ignores the possibility of an incident that would have only a local impact.

The Center for Infrastructure Assurance and Security (CIAS) decided to address this gap in the plan to secure the nations cyber infrastructures by creating a grass-roots level program that would help secure computer systems and networks at the local and state level, coordinating with federal agencies when appropriate. The first step in this effort was the creation of a community cyber security exercise for the city of San Antonio. Called Dark Screen, this exercise was conducted in September, 2002 and involved over 200 participants in a tabletop format. The event was a success in terms of making various leaders in the community aware of the potential for disruption that a cyber incident could cause. The participants included not just local city and county government leadership, but members from local utilities, federal agency representatives, and industry. All were made aware of the need to share information and to work together in the event of a cyber incident. As a result of the success of this event, the CIAS obtained funding to conduct similar events in other cities around the country. This occurred from 2003 through 2005.

At each community that the CIAS delivered an exercise in, the event seemed very successful in making the leadership aware of the potential problems a cyber incident would cause. After moving on to the next city, no further work was conducted with the city after the after action report was delivered. After two years, the CIAS began to take a look at the communities in which exercises had previously been conducted. What was discovered was that while the individuals in the community were aware that cyber incidents could be an issue, the communities had not taken any real step toward establishing a cyber security program. The cities were aware of the issues posed by cyber incidents, but they didn't know what to do in order to secure their own critical cyber infrastructures. This was not what had been expected and the CIAS determined that a new approach was needed.

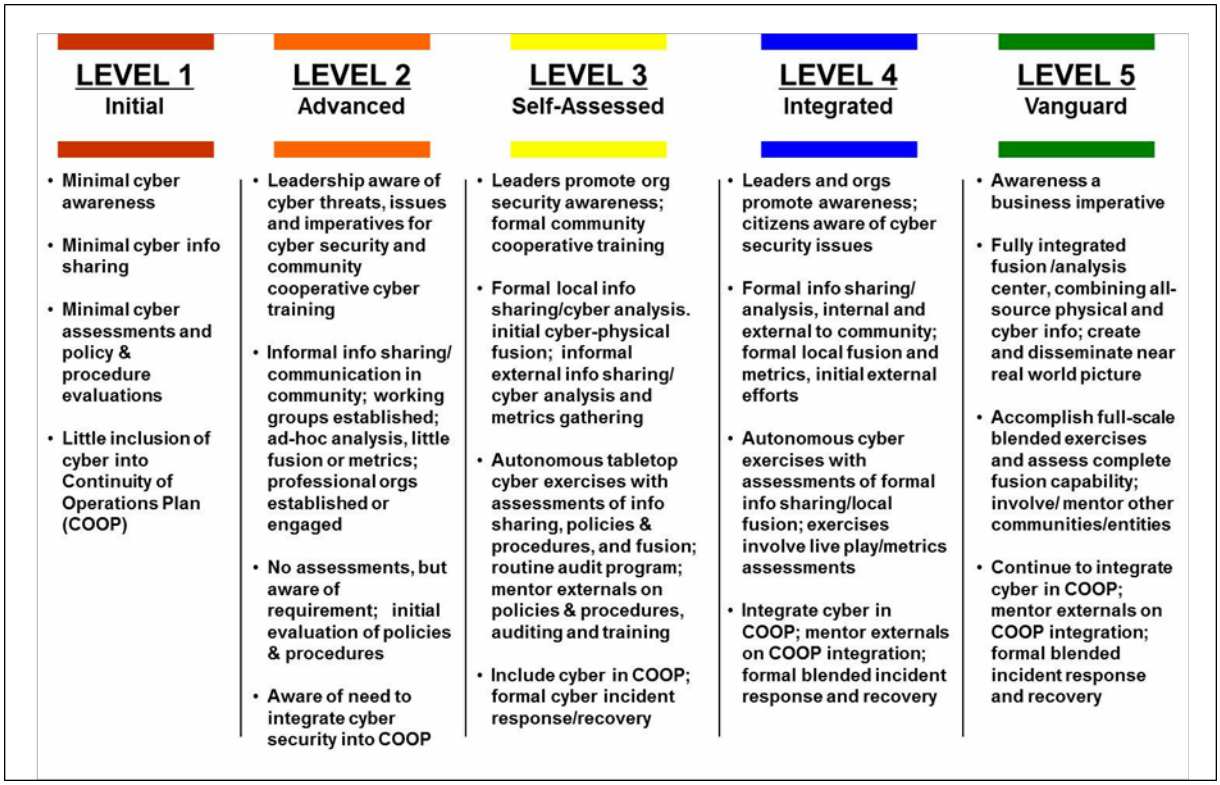


Figure F-1: The Community Cyber Security Model

4. Development of the CCSMM

The problem in the communities was that the leaders were still aware that a cyber incident could have a negative impact on the community, but they didn't know what to do in order to prepare for one or to address one should it occur. The first attempt to address this was to develop a course that would be provided to the community before the exercise. After the exercise, it was decided to provide some hands-on assistance to communities so that issues raised during the exercise could be addressed. These two additional events proved to be a tremendous step forward in helping communities as it helped them better understand what was needed. These two additions, however, were not enough as communities really needed a roadmap that they could follow to be able to build a viable and sustainable cyber security program. As a result, CIAS researchers came together and created the Community Cyber Security Maturity Model (CCSMM) to address this need. The model, as shown in Figure F-1, was designed to accomplish three things:

- Serve as a yardstick so that communities can determine where in the model they currently are (i.e. how mature their security program is)
- Serve as a roadmap so that a community knows what it needs to do in order to advance to the next level of the model.
- Provide a common point of reference so that different communities can discuss their respective programs and plans from a common perspective.

The model as shown describes the characteristics of communities at five levels of maturity. The first level basically describes a community that has not established cyber

security program. Unfortunately, in the experience of the CIAS, this has been the level that all communities are at. The next level, "advanced", describes a program that has advanced in its processes and has established the basics for a continued program. While the characteristics described at this level do not seem extremely difficult to attain, a community displaying all of these characteristics has actually taken a very large step toward establishing a cyber security program. The subsequent levels each build upon the basic characteristics as depicted here until at level 5, a community not only has a mature program but is also serving as an example and helping other communities attempting to establish their own programs. After several years of working with communities, it has been shown that it is possible for communities to establish programs based upon the model, but it will take years for a community to attain level 5.

One axis of the model shows the different levels a community can attain. The other axis describes what a community should have implemented in each of four characteristics. The first of these is awareness and describes how widespread the understanding of what the impact of a cyber incident might be on the community. The second is information sharing which describes what mechanisms are in place within the community to share information about and analyze cyber security events and what fusion efforts are performed to tie disparate pieces of information into a unified threat picture. The third characteristic describes what processes and procedures are in place in various organizations within the community to address cyber security. It also addresses what testing/exercise/practice is accomplished to evaluate the procedures that have been developed. The final characteristic describes to what extent cyber security is considered in the community's disaster planning process and what incident response steps have been implemented to cover a cyber incident.

5. Expansion of the CCSMM

The initial model developed was a tremendous first step in developing an approach to help communities establish viable and sustainable cyber security programs. Unfortunately, it soon became obvious that something was still missing. The main problem was that it was quickly realized that for a community to be mature enough in its program to reach the higher levels of the model would require a certain maturity for organizations within the community. In other words, for the community to be secure, the individual organizations within the community needed to also have a certain level of security. For a community to reach the upper levels of the model, it also needs to be able to rely on entities above it to provide certain assistance and information pre- and post-incident. Thus, for a community to be secure requires that the state also have a certain level of security program maturity. This meant the model was not a two-dimensional model as depicted in the Figure F-1 but should actually be a three dimensional model as shown in Figure F-2. This figure does not depict the intricate dependencies that exist between. Instead, it shows that, just like a community, organizations and states also have multiple levels for their programs. The model's name was not changed, even though it now encompasses more than just a community, because the focus is still on securing the nation from a community grass roots level.

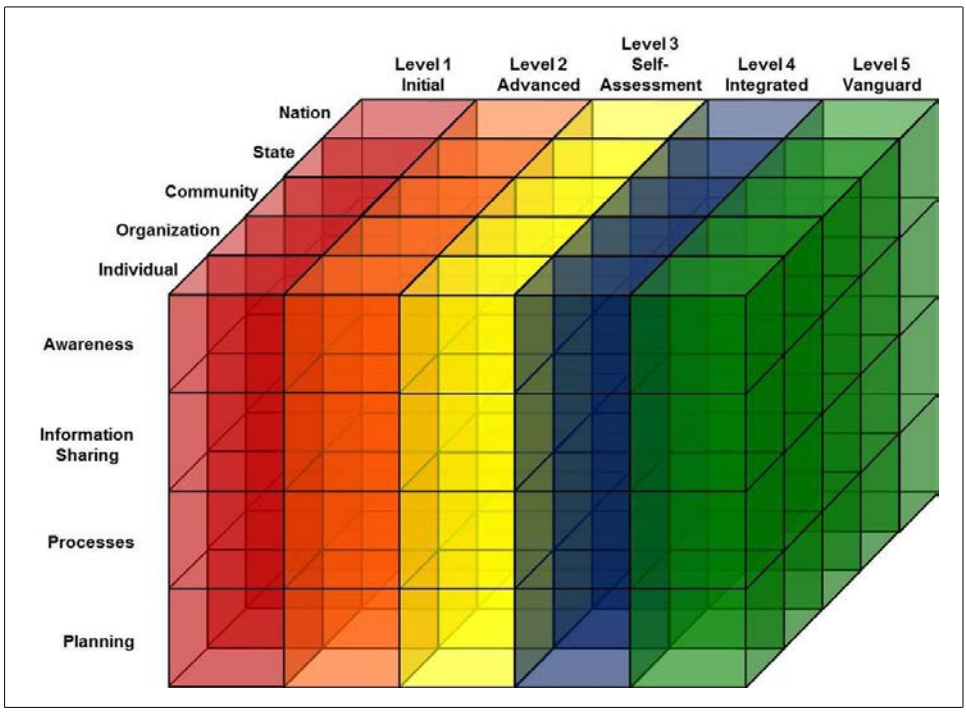


Figure F-2: The expanded 3-D model

While only the three levels of organization, community, and state are shown, other versions of this image include other levels that can be described – namely a national level, an international level, and an individual level. The individual level was a recognition that with the power of computer systems in the home today, individual citizens have a certain responsibility to secure their own systems so that they are not usurped and used, for example, in a distributed denial of service attack. Each of the boxes in the diagram can actually be expanded to describe the different parts of the model that are included at that level. In this image, instead of showing the characteristics at the various levels, the model shows the different parts that are part of a community's program at each level. This includes the metrics that are used to measure the current security posture of the community, the mechanisms that are in place to share information with other entities (whether in the community or upward to the state/nation), the training that is required or needed for "cyber first responders", the technology and tools that are needed to accomplish the different tasks that must be performed, the specific processes, procedures, and plans that exist (e.g. an incident response plan), and finally the types of tests and exercises that might be accomplished to evaluate how prepared the community is and how well the responsible "cyber first responders" understand their roles, duties, and responsibilities.

6. Conclusion

The Community Cyber Security Maturity Model, whose implementation has begun in five states within the United States, has shown to be a valuable tool in helping communities take an organized first step in establishing a viable and sustainable cyber security program. The model serves as a yardstick to determine the current level of maturity for a community, a roadmap for the community to follow in order to improve their security program, and a common point of

reference so that individuals in different communities can discuss their individual programs and share experiences and lessons learned. An expanded, three-dimensional version of the model actually illustrates the fact that the model can be expanded beyond the individual community perspective to encompass individual citizens, organizations, the nation, and multiple nations. Results from efforts in the five states the model is currently being implemented in have been very positive and participants in the various events that make up the program to implement the model have indicated that the information they have acquired in the program can be used to help implement programs within their organization and their state.

While much of the model has been developed, there still remain unknowns at the higher levels (since no community is currently at that level). In particular, the technology that will be required to ensure the security of a community in terms of its ability to effectively share information in a timely manner while maintaining the privacy and confidentiality of its citizens and organizations within the community is essential. Without sharing of information, the ability to detect in advance a pending attack will be significantly impacted. The goal should be to prevent attacks from occurring and not just responding to them. This will require a level of information sharing not currently present.

While initial indications are positive, the long-term impact of the program has not been determined since the program is still in its infancy. If communities are not able to sustain momentum then it must be determined what can be done to modify the program to ensure its effectiveness.

7. References

[1] Oregon.gov, "Oregon E-Government Program Benefits", www.das.state.or.us/DAS/EISPD/EGOV/benefits.shtml, June 14, 2011 .

[2] SPAMFighter, "Computer Virus Disrupts Houston Municipal Court System", www.spamfighter.com, 13 June 2011.

[3] Bradley Olson, Melissa Vargas, and Dale Lezon, "Computer virus shuts down Houston municipal courts", Houston Chronicle, Feb 7, 2009, 13 June 2011.

[4] FierceTelecom, "AT&T fiber optic cable cut in California", April 9, 2009, www.fiercetelecom.com, 13 June 2011.

[5] Malia Wollan, "California" Vandals Cut Phone Cables, Police Say", New York Times online, April 10, 2009, www.nytimes.com, 13 June 2011.

[6] Mike DeBonis, "Michigan prof explains how D.C. online voting system was updated.", Washingtonpost.com, voices.washingtonpost.com/devonis/2010/10, 13 June 2011.

[7] Matt Liebowitz, "Cop Car's Computer Hacked by Security Researcher", msnbc.com, 5/30/2011, www.msnbc.msn.com, 13 June 2011.

[8] Jaikumar Vijayan, "Web site offline as police, FBI investigate extortion bid," IT Health Care, May 7, 2009, 13 June 2011.

[9] Lifelock, "Virginia DHP Gets Their Data Held Hostage", May 5, 2009, 14 June 2011.

[10] Shalini Desai, "City's cyber crime website hacked.", July 12, 2010, www.mumbaimirror.com, 13 June 2011.

[11] Todd Datz, "SCADA System Security: Out of Control", csoonline.com, August 1, 2004, 14 June 2011.

Appendix G

Report Information Gathering Efforts

To arrive at a comprehensive understanding of the current cybersecurity environment in Texas, as well as determine consideration for recommendations, the Texas Cybersecurity, Education, and Economic Development Council (Council) utilized multiple approaches for gathering information. The following is a brief summary of the actions taken. Acknowledgement of participation by specific organizations and/or individuals can be found just prior to Appendix A.

- **Public Sector Survey** – The Council created an on-line survey that was distributed to over 5,000 individuals in Texas representing the following organizations: Local, State, Federal Agencies, Military Installations, K–12 School Districts, Higher Education Institutions, Health Science Centers, Hospitals, Ports, Telecommunications, Public Utilities: Electric, Natural Gas, Water, Chambers of Commerce and Emergency Services. The survey questions centered around the organizations' implementation of cybersecurity education programs and tactical strategy in the areas of people, process, and technology. The goal of the survey was to gauge the overall maturity of cybersecurity programs across the state as well as identify areas of common best practices.
- **Industry Survey** – A phone survey was conducted by Council members with corporate executives at private companies both within and outside of the state of Texas. Questions involved topics such as driving factors for corporate locations, barriers to investment, and cybersecurity concerns.
- **Interactive Dialogues** – Through a variety of face to face meetings, workshops, and seminars in multiple cities throughout Texas, the Council solicited information and feedback on items contained in the recommendations. These discussions addressed not only best practices to be included in the recommendations, but also provided advice on recommendations to be avoided.
- **Subject Matter Experts** – Leveraging the expertise available, the Council engaged cybersecurity experts from federal, state, and local agencies as well as private industry and higher education as a means of fully exploring the areas of recommendations. The experts participated in discussions regarding specific topic areas as well as red-team review of the draft recommendations.

Appendix H

Examples of Cybersecurity Incidents

Among cyber risks and threats to Texas business and their customers are:

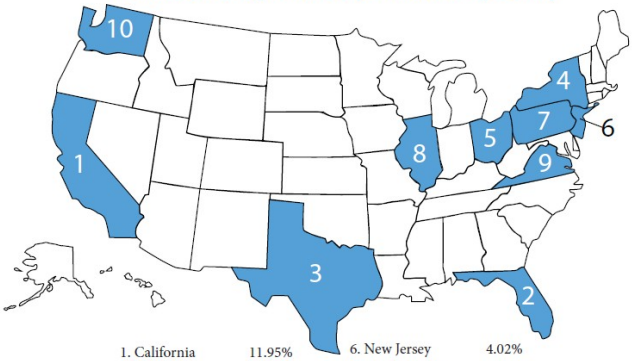
- **Loss of Privacy**: Texas has been subject to recently reported or discovered cyber incident events that violated customer privacy. Texas requires appropriate cybersecurity operations capabilities to assure the privacy of customer Social Security Numbers, Driver License Numbers, Credit Card data, private health information, and other personal data. According to the Identity Theft Research Center:
    - Of the 498 nationwide events in 2009 that exposed over 223 million customer records, 28 Texas events impacted nearly 70,000 customers;
    - Of the 662 nationwide events in 2010 that exposed over 16 million customer records, 35 Texas events impacted 140,000 customers;
    - Of the 419 nationwide events in 2011 that exposed nearly 23 million customer records, 31 Texas events impacted 8,780,000 customers;
    - Of the 212 nationwide events from January to June 2012 that improperly exposed over 8.5 million customer records, 13 Texas events impacted 90,000 customers.
- **Internet Crime:** Texas citizens have been subject to recently reported cybercrime events that placed them at risk of identity theft. Texas requires the ability to deliver cybersecurity awareness to Texas citizens of cyber threats to their identities that can cause them long term financial harm, and how they can protect themselves against cyber criminals. In the "2011 Internet Crime Report" produced by the Internet Crime Complaint Center:
    - Texas ranks third with the most individual complainants for being victims of Internet crimes (see Figure H-1 below).
    - While Texas did not appear in the Top 10 states based on per capita complaints, a significant number of Texans (18,477) filed as complainants of Internet crime.

Top 10 State Complainant Rates per 100,000 Population

State	Per 100,000 Population
1. Alaska	196
2. District of Columbia	137
3. New Jersey	131
4. Nevada	130
5. Colorado	123
6. Ohio	110
7. Maryland	109
8. Florida	107
9. Virginia	106
10. Washington	104

Note: Based on U.S. Census data.

Top 10 States by Count: Individual Complainants (Numbered by Rank)



1. California	11.95%	6. New Jersey	4.02%
2. Florida	7.01%	7. Pennsylvania	3.34%
3. Texas	6.46%	8. Illinois	3.07%
4. New York	5.27%	9. Virginia	2.96%
5. Ohio	4.43%	10. Washington	2.44%

Note: Of the complainants, 9.19% did not provide location information.

Source: Internet Crime Complaint Center

Figure H-1: Rankings of States in terms of Complaints Regarding Internet Crime

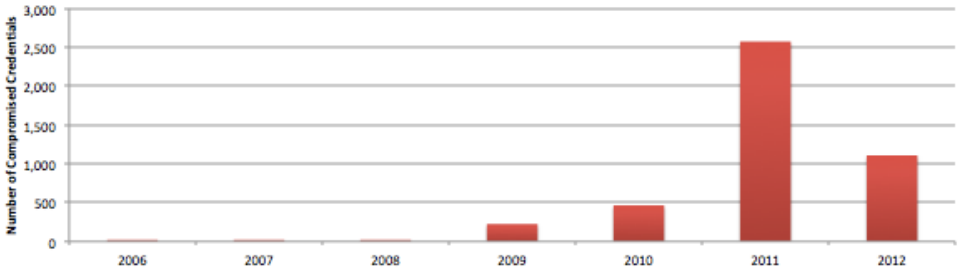
- **Intellectual Property Rights:** The Federal Bureau of Investigation has made preventing intellectual property theft a top priority of their cyber program – with a special focus on the theft of trade secrets and infringements on products that can impact consumers' health and safety. Texas needs an appropriate cybersecurity infrastructure to protect intellectual property belonging to nearly every Texas business organization including product designs and chemical formulae, sales and pricing strategies, strategic plans and financial data, and personnel and customer information. The FBI has noted a significant increase in nation states conducting intellectual property theft activity against U.S. businesses large and small – in fact they report they are "currently working over 400 such cases—many with a global nexus." The Texas cyber environment has been subject to recently reported cyber espionage events that placed Texas business at financial risk.
    - A former Houston-based Dow Chemical scientist was arrested in 2008 and later convicted for stealing and selling trade secrets worth millions of dollars to China.
    - Two Houston based men who admitted that that manufactured and sold oilfield pipe couplings improperly stamped with the American Petroleum Institute (API) certification mark with many of those couplings made using substandard materials.
    - A U.S. citizen residing in Houston plead guilty to theft of trade secrets in April 2012 and admitted he illegally copied and downloaded intellectual property, specifically product data sheets, belonging to his employer in an effort to economically benefit himself.
- **Critical Infrastructure Outages**: The U.S. federal government has recognized that massive power outages caused by cyber events could disrupt the nation's economy. The U.S. Industrial Control System Cyber Emergency Response Team that monitors control system vulnerabilities notes a significant increase in attempted cyber-attack against U.S. public and private critical

infrastructure companies - nine incident reports in 2009, 41 incident reports in 2010, 198 incident reports in 2011. Texas critical infrastructures support strategic state capabilities such as electricity generation, transmission and distribution; gas production, transport and distribution; oil and oil products production, transport and distribution; telecommunication; water supply (drinking water, waste water/sewage, surface water); agriculture, food production and distribution; heating (e.g. natural gas, fuel oil, district heating); public health (hospitals, ambulances); transportation systems (fuel supply, railways, airports, harbors, inland shipping); financial services (banking, clearing); and security services (police, military). These infrastructures contain many legacy or older systems that cannot be easily replaced or updated to make them more resilient to cyber threats. Some high profile cyber events impacting critical infrastructure include:

- Cyber-attacks that caused power outages in parts of Brazil in January 2005 and September 2007;
- Over 1 million Texans being impacted by weather related power outages in February 2011;
- An Iranian natural gas pipeline that exploded and along with a main oil exporting facility, were shut down in 2011 by cyber-attacks;
- Anonymous computer hacking activists allegedly breaching computer systems of major energy companies including Shell, BP Global, ExxonMobil, Gazprom, and Rosneft in June and July 2012 to protest offshore drilling in the arctic.
- Power outages in July 2012 leaving 600 million people without power, bank ATMs, or traffic lights, and impacted companies and entities lacking emergency power or other continuity capabilities.

- **Large Corporation Exposure:** Fifty-two Fortune 500 companies operate their headquarters within the state of Texas and hundreds more perform considerable business within the state. A rising corporate threat to large organizations is the exposure – through breach, phishing, or cybercrime – of their employee usernames, passwords, and credentials. Several high profile breach events in 2012 as well as many more that are unreported involved access by a hacker to personally identifiable information and/or financial information that is housed within these organizations:

  - Experian exposure through Texas credit union: Cyber-thieves broke into an Abilene Telco Federal Credit Union employee's computer and stole the password for the bank's online account with Experian plc, the credit reporting agency with data on more than 740 million consumers. The intruders then downloaded credit reports on 847 people, taking Social Security numbers, birthdates and detailed financial data on people across the country who had never done business with Abilene Telco.
  - The number of compromised credentials leaked from Texas-based Fortune 500 companies has increased 395% since 200.



Compromised Credentials	4,337	Texas-based Fortune 500 Companies	52
Credentials with Credit Cards	341	Texas-based Fortune 500 Companies with Compromised Credentials	37
Credentials with SSNs	17	Percentage of Texas-Based Fortune 500 Companies with Compromised Credentials	71%

Source: CSID Independent Analysis – 2012

Figure H-2. Compromised Credentials for Texas-based Fortune 500 Companies (2006–2012)

- **Malware and Botnet Operation**: Malware poses one of the most significant threats to individuals and organizations within the State of Texas due to the inherent ability to infect computers at large scale in order to record sensitive information such as keystrokes and screenshots and subsequently exfiltrate that data to a command and control server for harvesting and redistribution. Texas has also been a source for cybertheives hosting botnet command and control servers and propagating malware:
    - The federal government shut down massive Coreflood botnet run out of North Texas and elsewhere, substituting its own servers for criminal's servers to identify victims and send warnings to ISPs.
    - The specific botnet, Coreflood, is a particularly harmful type of malicious software that records keystrokes and private communications on a computer. Once a computer is infected with Coreflood, it can be controlled remotely from another computer. According to information contained in court filings the group of all computers infected with Coreflood is believed to have been operating for nearly a decade and to have infected more than two million computers worldwide.

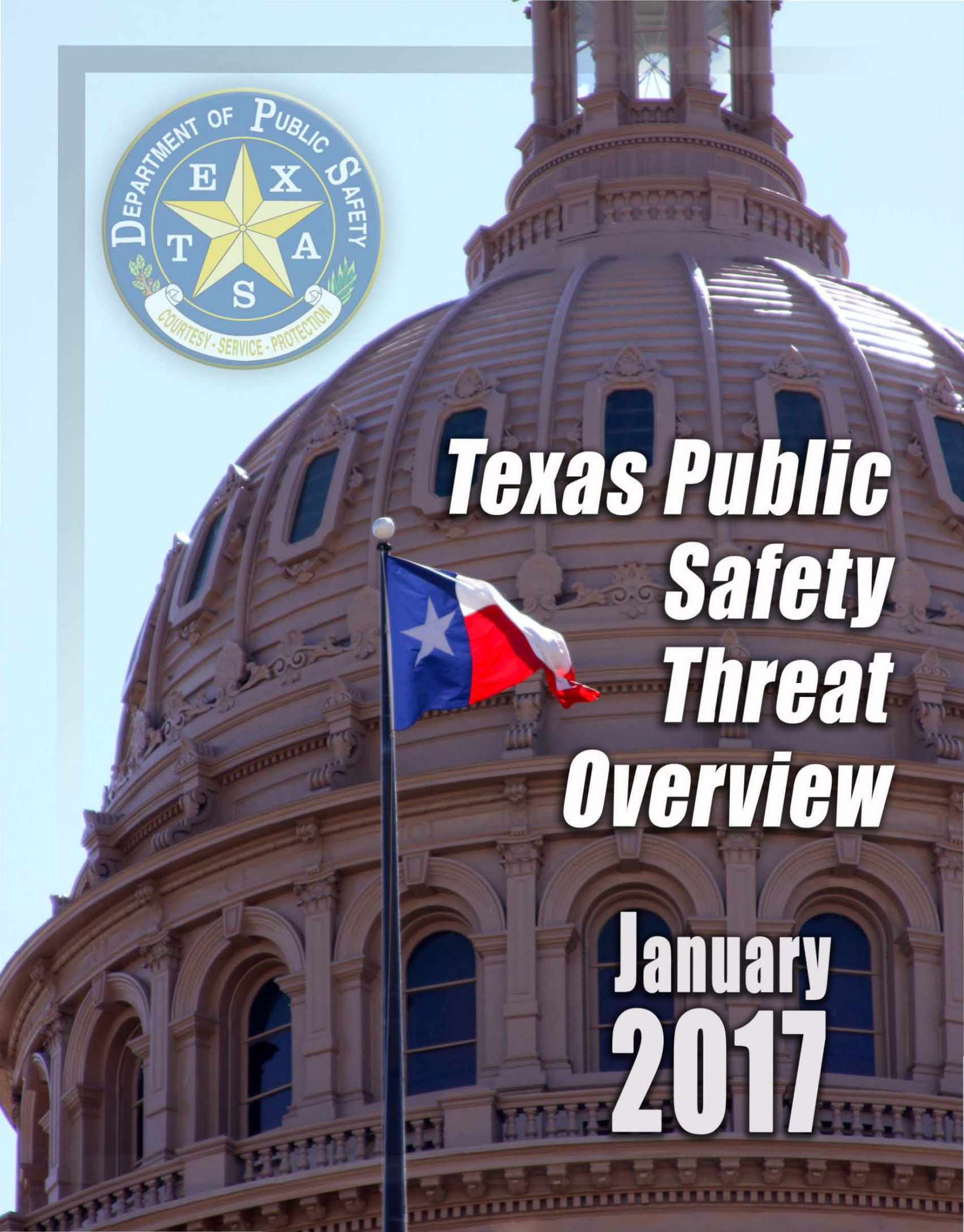
Appendix I

Resources and References

The Council examined a number of documents in order to draw from the experience of other studies in related areas. These documents provided much insight into the issues surrounding the challenges faced in Texas and a list of some of the more pertinent documents and where they can be obtained follows:

- "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency" http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf
- "A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters. A Report of the CSIS Commission on Cybersecurity for the 44th Presidency" http://csis.org/files/publication/100720_Lewis_HumanCapital_WEB_BlkWhteVersion.pdf
- "Cybersecurity Two Years Later. A Report of the Commission on Cybersecurity for the 44th Presidency" http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf
- "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure" www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
- "Department of Defense Strategy for Operating in Cyberspace"
- "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World." www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
- "Report of the State Infrastructure Protection Advisory Committee (SIPAC)"
- "State Enterprise Security Plan: Securing Texas Information Resources" www2.dir.state.tx.us/SiteCollectionDocuments/Security/Policies and Standards/StateEnterpriseSecurityPlan.pdf
- State of Texas Information and Computer Technology Cluster Assessment www.texasindustryprofiles.com/PDF/twcClusterReports/TexasITCluster.pdf
- Texas Homeland Security Strategic Plan: 2010–2015 http://governor.state.tx.us/files/homeland/HmLndSecurity_StratPlan2015.pdf

For more about the
Texas Cybersecurity, Education, and Economic Development Council,
please see www.dir.texas.gov/sponsored/sb988/pages/overview.aspx.



Texas Public Safety Threat Overview

January 2017

Texas Public Safety Threat Overview

A State Intelligence Estimate

Produced by the Texas Department of Public Safety

In collaboration with other law enforcement and homeland security agencies

January 2017

Executive Summary

(U) Texas faces the full spectrum of threats, and the state's vast size, geography, and large population present unique challenges to public safety and homeland security. Texas employs a systematic approach to detect, assess, and prioritize public safety threats within seven categories: terrorism, crime, motor vehicle crashes, natural disasters, public health threats, industrial accidents, and cyber threats.

(U) Due to the recent actions of lone offenders or small groups affiliated with or inspired by the Islamic State of Iraq and Syria (ISIS) and other foreign terrorist organizations, we assess that the current terrorism threat to Texas is elevated. We recognize that ISIS has had considerable success in inspiring and inciting lone offenders to attack targets in the United States and other Western countries using simple yet effective tactics that are difficult to detect and disrupt. We expect this heightened threat to persist over at least the next year, due in part to the relatively high number of recent terrorism-related arrests and thwarted plots inside the US, and the prevalence and effectiveness of ISIS's online recruitment and incitement messaging, as the organization is slowly defeated on the battlefield. We are especially concerned about the potential for terrorist infiltration across the US-Mexico border, particularly as foreign terrorist fighters depart Syria and Iraq and enter global migration flows. We are concerned about the challenges associated with the security vetting of Syrian war refugees or asylum seekers who are resettled in Texas – namely, that derogatory security information about individuals is inaccessible or nonexistent. We see a potential that these challenges may leave the state exposed to extremist actors who pose as authentic refugees, and who are determined to later commit violent acts.

(U) Other threats, such as those from violent domestic antigovernment extremists, remain concerning in light of standoffs with federal law enforcement in Oregon in 2014 and Nevada in early 2016, as well as a series of ambush murders of police officers.

(U) Crime threatens the public safety and liberty of all Texans in some way. The Texas Department of Public Safety's (DPS) Uniform Crime Reporting (UCR) program data for 2015 shows a 4.7 percent decrease of the major crime rate in Texas from 2014. This is positive for the safety and welfare of our citizens. Conversely, violent crimes in particular increased for the second year in a row. Texas' UCR program includes seven index crimes: homicide, rape, robbery, aggravated assault, burglary, larceny, and motor vehicle theft. What the index crime data does not currently account for are other crimes typically committed by criminal organizations that impact the security of Texas communities, such as human trafficking, drug trafficking, kidnapping, extortion, money laundering, and public corruption. Mexican cartels, human traffickers, street and transnational gangs, human smugglers, and high-threat criminals are all major criminal threats to Texas.

(U) Criminal organizations – including Mexican cartels and transnational gangs – and individual criminals engage in a wide range of illicit activities in Texas. Among the vilest crimes these organizations and other criminals engage in is the exploitation and trafficking of children and other vulnerable victims. Human trafficking is highly profitable, and is the fastest growing organized crime business in Texas. It involves the recruitment, harboring, transporting, or procurement of a person for labor or services involving involuntary servitude, slavery, or forced commercial sex acts. These crimes are also carried out and enabled by human smugglers, prostitution rings, manufacturers and consumers of child pornography, and sexual predators.

(U) All eight of the major Mexican cartels operate in Texas, and they have enlisted transnational and statewide gangs to support their drug and human smuggling and human trafficking operations on both sides of the border.

(U) Gangs continue to pose a significant public safety threat to Texas, and their propensity for violence and many kinds of criminal activity is persistent. While the greatest concentrations of gang activity tend to be in the larger metropolitan areas, gang members are also present in the surrounding suburbs, and in rural areas. Gang activity is especially prevalent in some of the counties adjacent to Mexico and along key smuggling corridors, since many Texas-based gangs are involved in cross-border trafficking.

(U) Motor vehicle crashes killed 3,520 people in Texas in 2015. In addition, the high volume of commercial motor vehicles on Texas' roadways, including those that operate unsafely and violate the law, is a particular concern because of the increased potential for loss of life when large-mass commercial vehicles are involved in crashes.

(U) Texas faces an array of natural threats, including floods, hurricanes, wildfires, tornados, and drought, with more major disaster declarations than any other state in the nation. These disasters result in loss of life, damage to infrastructure, and billions of dollars in personal property damage and economic losses.

(U) Public health threats to Texas remain a significant concern, with emerging infectious diseases and other illnesses such as influenza and enteroviruses. In September 2014, a Texas hospital patient tested positive for the Ebola virus following his recent travel to West Africa, making him the first case diagnosed in the United States. Texas worked with public health professionals across the state to contain Ebola cases and prepare for other potential infections, but the virus's emergence served as a reminder that foreign-borne diseases can be brought to Texas.

(U) Major industrial accidents constitute another potential threat to public safety, especially because of the large industrial base in Texas. The state's vast size and economic importance contribute to the potential for severe consequences if any significant accidents occur.

(U) Since technology has become a target, a vulnerability, and a tool used by criminals and foreign governments, cyber threats continue to be a significant area of concern, and we are especially concerned about the potential consequences of a successful cyberattack on the state's critical infrastructure.

Table of Contents

Acknowledgments

(U) The Texas Department of Public Safety collaborated with law enforcement, homeland security, and other government agencies across Texas and the United States in the production of this State Intelligence Estimate to serve as a high-level overview of the public safety threats to Texas. Their contributions were invaluable to developing an assessment of the main threats in Texas. This collaboration underscores the commitment among agencies across the state to share information, intelligence and capabilities to effectively address public safety threats across all jurisdictions and disciplines at all levels. We are grateful to the numerous agencies that contributed to this assessment.

State Intelligence Estimates

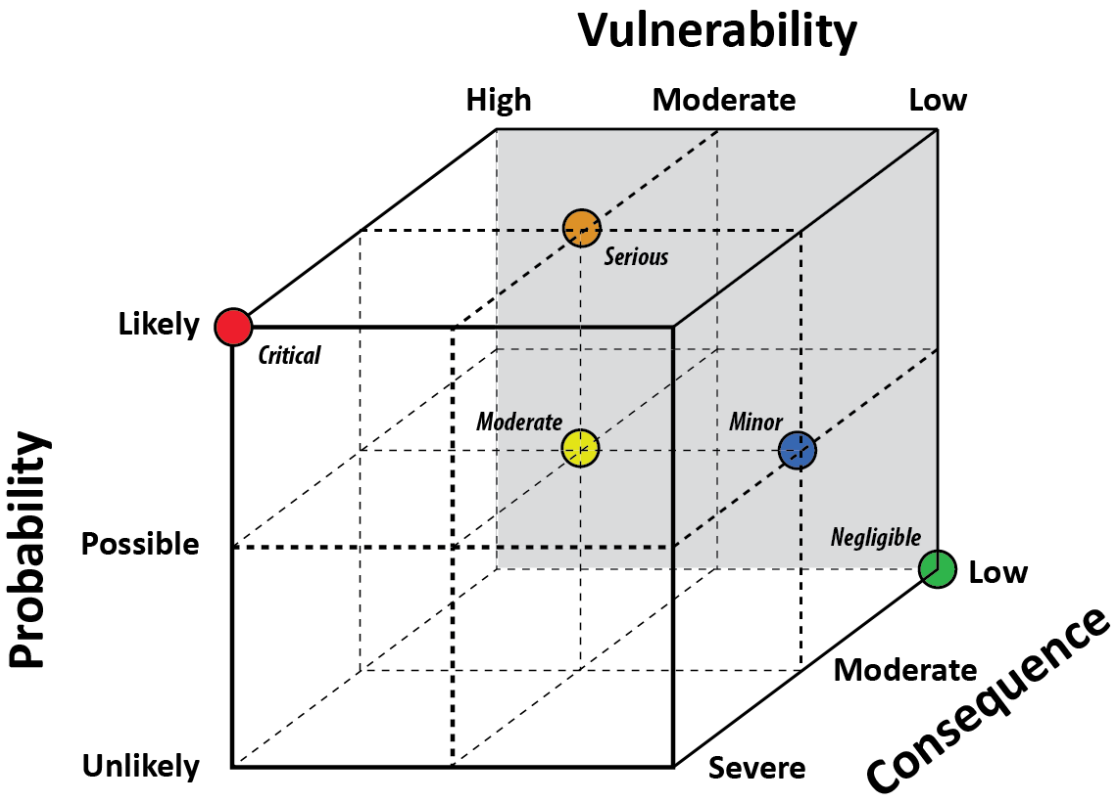
(U) To enhance the state's ability to detect, assess, and prioritize threats to the safety and security of its citizens, the Texas Department of Public Safety implemented a State Intelligence Estimate process after consultation with the National Intelligence Council, based in part on the model of the National Intelligence Estimate.

(U) State Intelligence Estimates are multi-agency assessments on issues relating to homeland security and public safety in Texas. They serve as the most authoritative and comprehensive analyses of these issues, and they are designed to provide law enforcement and government officials with the most accurate evaluation of current information on a given topic. State Intelligence Estimates are intended to provide an assessment on the current status of an issue, but they may also include estimative conclusions that make forecasts about future developments and identify the implications for Texas.

(U) Unlike reports and assessments produced by an individual agency or center, State Intelligence Estimates draw on the information and expertise of multiple law enforcement and homeland security agencies across Texas. Such an approach is essential to developing a comprehensive assessment of issues that affect the state as a whole. By incorporating the perspectives and information from multiple agencies, the Texas Department of Public Safety is better able to produce assessments that support the development of proactive strategies and policies needed to address current and evolving threats to the state.

Introduction

(U) Proactive and preventive strategies require sufficient data and analysis to support tactical and strategic decision making at all levels in today's rapidly evolving threat environment. Texas employs a systematic approach to detect, assess, and prioritize public safety threats within seven categories: terrorism, crime, natural disasters, motor vehicle crashes, public health, industrial accidents and cyber threats. Aligning threats within categories facilitates threat analysis and prioritization. Texas employs three risk variables that are commonly used in risk models: Probability, Vulnerability, and Consequence. These are used to assess the current or likely threat, in a formula that is expressed as Threat = Probability x Vulnerability x Consequence.



(U) In this standard model, Probability takes into account the frequency or likelihood that a harmful event or condition will occur. Vulnerability considers the extent to which the state is susceptible to a harmful event or condition. Consequence represents the impact that the harmful event or condition is likely to have on the state if it does occur. This threat assessment framework is particularly useful in delineating those threats that are high consequence and low probability from those that are more likely and that have comparatively moderate consequences. For example, the vulnerability of the Houston Ship Channel to a Category 4 or 5 hurricane is high and the consequences substantial, and even though the probability of it occurring is low based on historical trends, a comprehensive and well-rehearsed regional response plan is essential to minimizing the danger. This matrix represents the threat assessment process, though the report does not maintain scores for individual threats and threat categories.

Threat Overview

(U) Texas faces the full spectrum of threats and hazards. The globalization and convergence of crime and terrorism; an unsecure border with Mexico, powerful and ruthless Mexican cartels, violent transnational and statewide gangs, and serial criminals; worldwide terrorist organizations and lone-offenders; cyber intrusions and threats; the unpredictability of catastrophic natural disasters and pandemic diseases; the high loss of life from vehicle crashes; the large amount of nationally significant critical infrastructure in Texas, and the dramatic and continued increases in the state's population – all of these factors have resulted in an asymmetric threat environment in our state that requires constant vigilance to minimize the danger to our citizens and their families.

Overlay Map of Texas on the Northeastern United States

(U) Texas has 29 ports of entry, 1,254 miles of international border with Mexico, 367 miles of coastline and over 267,000 square miles of landmass, making it larger than France and twice the size of Germany. It is larger than many US states combined. El Paso is closer to San Diego, California and Houston is closer to Tallahassee, Florida than El Paso and Houston are to one another.

(U) Texas is also demographically diverse, with a large population that is quickly growing. The state's near 27.5 million residents are concentrated in large urban and suburban areas, but are also spread across vast rural areas. More than 7.1 million people live in the Dallas-Fort Worth-Arlington metropolitan area, and 6.6 million in the Houston-Woodlands-Sugarland metropolitan area. At the other end of the spectrum, several Texas counties have small populations with fewer than 1,000 people. Texas' vast distances create challenges with regard to communications and capabilities.

(U) Finally, Texas has a large and diversified economy, with a gross domestic product of more than $1.4 trillion. Texas accounts for significant volumes of international trade with Mexico and other nations. The state also plays a vital role in the nation's agriculture, defense, and energy industrial activity. Some of these industries and associated facilities have been designated as nationally important critical infrastructure. Appendix 1 provides an overview of critical infrastructure sectors and their importance.

1. Terrorism

(U) We assess that the current terrorism threat to Texas is elevated in light of the relative frequency of recent attacks and thwarted plots in Europe and in the US, organized, supported, or inspired by the Islamic State of Iraq and Syria (ISIS) and other foreign terrorist organizations. At issue is that ISIS and other terrorist groups, from afar, have succeeded in using various methods, including online propaganda and incitement messaging through social media, to inspire lone offenders and small groups to attack targets in the United States and in Europe. These inspired offenders, sometimes using the simple yet effective tactics laid out for them, are highly difficult to detect and disrupt. The incitement capability for such attacks was indicated, for instance, when two Arizona extremists, already considering various targets, noticed social media reporting about a "Draw the Prophet Mohammed" contest in Garland, Texas. In May 2015, two extremists drove to the Garland event and launched an attack at the contest location – as extremists abroad had been vigorously urging American ISIS loyalists to do.[1] [2] [3] A few months later, in San Bernardino, California, two local attackers killed 14 people after reportedly pledging allegiance to ISIS.[4] In June 2016, a lone offender in Florida, also likely inspired in part by the group, killed 49 people and wounded 53 others inside an Orlando nightclub.[5]

(U) To assess the threat most accurately, we also consider the number of attacks that were attempted but thwarted, rather than merely the relative few that succeeded or the number of their victims. In the past two years, federal authorities have arrested more than 90 ISIS supporters inside the United States, and have broken up dozens of plots among them to commit violent acts inside the country.[6]

(U) The group's deployment of trained operatives for attacks outside of its territory in Syria and Iraq, particularly in Europe, is relatively new. The strategy appears to have intensified amid ISIS territorial losses in those countries due to oppositional military pressure. The group's external multi-location attack strategy as it loses territory is of particular concern to the US by the continuing volume of ISIS-inspired or supported attacks and plots, have been attempted or carried out in France, France, Belgium, Germany, Turkey, at a café in Bangladesh frequented by international customers, in The Philippines, and elsewhere where loyalist affiliates have arisen. Additional terrorist attack plots have been foiled in Europe since July 2016, when another ISIS operative in France, supported by a cell, murdered 86 people, including two Texans, by driving a truck through crowds of people celebrating Bastille Day in Nice.

(U) The many attacks and thwarted plots in France, Belgium and in Germany underscore the persistent threat posed by returning foreign fighters in general. But those high-casualty European attacks also relied, seemingly for the first time, on the use of illegal migration and human smuggling tactics by which ISIS infiltrated the returning fighters into Europe-bound migration flows, which may hold implications for the US-Mexico border.[7] [8]

(U) Some of the operatives who carried out the 2015-2016 France and Belgium attacks reportedly were returning foreign terrorist fighters of French and Belgian citizenship who posed as illegal immigrant asylum seekers as they arrived at land borders. Also, a number of non-citizen migrant asylum seekers, rather than returning citizens, were involved in later attacks and plots.[9] [10] [11] [12] [13] [14] For example, European counterterrorism authorities arrested a Syrian refugee planning a bombing attack in Germany,[15] three Iraqi migrants in Switzerland,[16] and several Afghan migrants in Italy in the midst of attack planning.[17] A Syrian asylum-seeking migrant ISIS sympathizer was shot dead after he attacked a Paris police station.[18] Among many other such cases of extremist migrants, a recent immigrant attacked people on a commuter train in Germany, where counterterrorism police reportedly identified at least 40 other migrant, border-crossing asylum seekers suspected of terrorism.[19]

(U) Given how ISIS deployed operatives to their targets in European capitals via long-distance and illegal immigration methods, we recognize the potential that ISIS and other groups have noted the successful use of this tactic and would contemplate infiltrating operatives in the same manner across the Texas-Mexico border, possibly also posing as asylum seekers. We recognize that millions of migrants not associated with terrorism had overwhelmed European border controls in comparison. However, we note that human smugglers, working along established Latin American routes, have long transported Syrians, Iraqis, and other immigrants from countries where terrorist groups operate to our land border with Mexico, where they often seek asylum too. [20] As well, migrants from countries with a known terrorism presence – known as "special interest aliens" (SIAs) – have included travelers from Turkey, Iran, Afghanistan, Pakistan, Lebanon, Egypt and many other "countries of interest" in the Middle East, North Africa and South Asia where terrorist groups are active. These immigrants sometimes seek asylum fraudulently at the Texas-Mexico border, as did the terrorist-immigrants upon reaching Europe.[21] [22] [23] [24] [25] [26] [27] [28] [29]

(U) Our concern extends also to the issue of refugee resettlement and the thoroughness of vetting, given some past instances in which refugees from the Middle East region have been prosecuted inside the United States for terrorism. For example, in January 2016, Houston resident and Iraqi-born refugee Omar Faraj Saeed Al-Hardan was indicted on three felony offenses related to plans both to join ISIS overseas and also to bomb two Houston malls. Al-Hardan entered the US as a legal resettled refugee in November 2009 and was granted legal permanent resident status in August 2011.[30]

(U) We expect the threat from ISIS-inspired homegrown violent extremists, returning foreign fighters, and external attack plots to persist over at least the next year as the terrorist organization suffers ongoing military defeats in Iraq. We reach this judgment due in part to the group's ongoing external attack campaign, continuing online incitement messaging capability, and the movement of foreign fighters from ISIS-influenced terrorist redoubts outside of Iraq and Syria.[31]

(U) We also recognize the persistent threat posed by al-Qaeda, its affiliates, and other foreign terrorist organizations, such as the Pakistani Taliban, which continue to articulate their aspirations to attack the US, particularly as al-Qaeda tries to strengthen its global networks as ISIS loses territory.

(U) Other threats, such as violent domestic extremists, also remain a concern, as evidenced by the July 2016 shootings of 20 Dallas and Baton Rouge law enforcement officers, as well as the November 2014 shooting attack on multiple targets in downtown Austin by a man who identified with a white supremacist ideology known as the "Phineas Priesthood."

1.1 ISIS Contributing to Current Heightened Global Terrorism Threat

(U) We judge that the global threat of terrorism in Texas and the US has increased substantially over the past two years— attributable, in part, to ISIS's June 2014 seizure of northern Iraq. This territory seizure afforded the terrorist organization protected human resources and revenue, a safe haven from which to plot attacks, and the narrative of an expanding caliphate. Despite the significant progress of various military efforts to shrink ISIS territory in Iraq, we judge that the group's capacity to operate as a terrorist organization with global capabilities can continue for some time from other regional hubs in the Middle East, Africa, Afghanistan, and South Asia. This assessment is based on currently available data, intelligence and statements of heightened concern by senior leadership within the US Intelligence Community, including the following reporting:[32] [33] [34] [35] [36]

- (U) Between October 2014 and July 2016, attacks attributed to ISIS outside of Syria and Iraq killed more than 1,200 people in approximately 17 countries.[37] [38] [39]

- (U) Since 2014, there have been at least seven attacks attributed to ISIS-inspired terrorists in North America, with five in the US, including one in Texas. Attacks actually carried out include the June 2016 Orlando nightclub massacre and the January 2016 shooting of a Philadelphia police officer, both by men claiming to have acted on behalf of ISIS.[40]

- (U) The number of successful attacks stands in contrast to historically elevated numbers of US terrorism attack plots that were thwarted before they could be carried out, which indicates a more complete picture of the persistence of effort. In just the first half of 2016, law enforcement investigations have resulted in the arrests or indictments of at least 48 individuals in the United States in ISIS-related cases.[41] The cases involve individuals plotting attacks; attempting to travel to join ISIS overseas; sending money, equipment and weapons to terrorists; falsifying statements to federal authorities; and failing to report a felony. Also, as of mid-2016, the FBI had nearly 1,000 open investigations across most of the US states.[42]

- (U) In July 2016, FBI Director James Comey and CIA Director John Brennan warned that hundreds of terrorists will fan out to infiltrate Western Europe and the US to carry out attacks on a wider scale as ISIS is defeated in Syria and Iraq, and that efforts to that date had not reduced the group's capability and global reach.[43]

1.1.2 ISIS Inciting Lone Offender Attacks Through Social Media

(U) Some terrorist organizations have been particularly effective at using social media and online messaging to communicate with and inspire sympathizers around the world to attack Western targets. We assess that ISIS incitement propaganda– which includes videos, social media posts, and online magazines – likely has inspired sympathizers to engage in violent attacks on their own. ISIS's ability to generate timely new propaganda has grown, resulting in the online publishing of hundreds of official ISIS products.[44] [45] Lone offender or small group attacks, often inspired at least in part by ISIS, pose substantial challenges for law enforcement to detect indicators of a pending attack. Many such attacks have involved limited visible pre-operational planning and communication and used simple tactics with readily available weapons – such as firearms, edged weapons and vehicles. Examples of apparently externally inspired attacks that went undetected over the past two years include:

- (U) The June 12, 2016 small-arms attack by a lone offender on an Orlando nightclub in which 49 people were killed and others were held hostage for hours before police killed the gunman. [46] Officials said the gunman had been inspired in part by ISIS messaging.[47]

- (U) The May 3, 2015 small arms attack by two radicalized individuals on a Garland, Texas Muhammad Art Exhibit & Contest event, amid social media calls for an attack on the event. Police killed the two gunmen as they began a firearms attack just outside the event.[48]

- (U) The December 2, 2015 attack on county government personnel by a radicalized husband-wife team at the Inland Regional Center in San Bernardino, California, who killed 14 and wounded dozens before they were killed after a running gun battle. The attack occurred amid an extended ISIS social media incitement campaign for attacks on government workers of all kinds.[49]

- (U) The January 14, 2015 arrest of an Ohio man for conspiring to kill a federal officer and attacking the US Capitol, following the suspect's reposting of online statements supporting ISIS and video propaganda sympathizing with violent "jihad" on a social media account.[50]

- (U) The October 22, 2014 attack by an Algerian-Canadian man at the National War Memorial in Ottawa, Canada, in which he shot and killed a Canadian soldier after ISIS propagandists called for retaliation in response to new Western airstrikes. The suspect was described as having converted to Islam and self-radicalized.[51] This attack followed an incident two days earlier when a different radicalized Canadian national struck two Canadian soldiers with an automobile outside a military facility in Quebec, killing one soldier and wounding the other, a method expressly called for in ISIS social media incitement.[52]

(U) In addition, sympathizers of these groups also regularly use social media and online forums to promote recent attacks and encourage new ones.[53] Following the November 2015 Paris attacks, for instance, terrorist sympathizers used Twitter accounts to urge similar attacks on American cities.[54] Further examples of post-attack messaging include:

- (U) An incitement campaign, including al-Qaeda's *Inspire* magazine and many extremist social media forums, based on the September 2014 beheading of a co-worker in Moore, Oklahoma by a suspect who believed non-Muslim co-workers had religiously oppressed him. His Facebook page featured photos of a beheading in Syria, rebel fighters, and Quran verses justifying attacks.

- (U) *Inspire* magazine quoted and praised Mohammed Ali Brown, the Seattle suspect in the murder of four people in New Jersey and Washington State over several months in 2014. According to media reporting, the suspect shot random men at close range late at night in quiet locations, in retaliation for US foreign actions in which Muslims had been killed.[55] [56]

- (U) An issue of ISIS's *DABIQ* magazine praised an October 2014 hatchet attack on a group of New York City police officers that left two officers wounded. [57] The suspect reportedly was a self-radicalized convert to Islam who had posted comments on Facebook and YouTube supporting violent attacks inspired by terrorist groups like ISIS.[58]

- (U) *Inspire* magazine commended the October 2014 hatchet attack on a Washington, D.C. police officer that took place one week after the New York City attack. In this case, the unidentified suspect swung a hatchet at a police officer and fled after a brief struggle.[59]

1.1.3 Calls for "Assassination" Attacks Targeting Law Enforcement, Government, and Military Personnel, Religious Leaders, and High-Profile Civilians

(U) ISIS, other foreign terrorist organizations, and their sympathizers have singled out groups and individuals as desirable assassination targets. In the United States and other Western countries, these targets most often include news media, law enforcement, and military personnel, as well as government facilities and public places such as shopping centers. Given successful ISIS assassination operations abroad and the disrupted May 2015 attack in Garland, we are concerned about the influence of these messages and the potential for successful lone offender attacks on targets in Texas. Recently, propagandists have mentioned Texas and have released "kill lists" identifying Texas residents in their messaging, including:

- (U) In May 2016 via the messaging app Telegram, the pro-Islamic State hacking group United Cyber Caliphate posted a list of 1,543 names, personal addresses, and IP addresses belonging to Texas residents described as "most important crusaders in Texas" who are "wanted to be killed." The message encouraged would-be attackers to "crush the cross" and "shoot them down."[60] Later "kill lists" containing the names of hundreds of Texas residents have been released as well.

- (U) In December 2014, *Inspire* magazine referenced Texas in a call for the state's Muslim residents to conduct lone offender attacks. The publication identified Texas and eight other states for their significant Muslim populations, noting that "9000+ 'Muslims' are on active duty in the US Army." Other states listed were California, New York, Illinois, New Jersey, Michigan, Virginia, Ohio, and Maryland.

(U) More generally, terrorist propagandists urge US-based sympathizers to attack targets of opportunity anywhere in the US, including in Texas. For example:

- (U) In January 2015, a pro-ISIS media group in an Islamist extremist forum that promoted attacks listed Dallas, Texas, among locations where "Cesium-131 poison spreads on your streets and train stations…" Other locations that were named included Boston, Virginia, Russia, and Amsterdam.

- (U) The Spring 2014 issue of *Inspire* magazine listed Houston and Dallas among desirable US cities to target.

- On February 21, 2015, the Somali-based al-Shabaab released a predominately English-language video highlighting the September 2013 terrorist attack on the Westgate Mall in Nairobi, Kenya. The video encouraged similar attacks on "American or Jewish-owned" shopping centers and districts.

- (U) On January 10, 2015, ISIS released a video via social networking sites reiterating the group's encouragement of lone offender attacks in Western countries. The video highlighted excerpts from a September 2014 audio message attributed to an ISIS spokesman advocating for attacks against "soldiers, patrons, and troops…their police, security, and intelligence members."

- (U) On January 14, 2015, a video released on the official Twitter account of an ISIS division praised the attacks on *Charlie Hebdo* magazine offices in Paris, France. The video showed three French-speaking fighters calling for additional attacks in Europe and the US. One fighter advised those unable to travel to ISIS territory, "If you see a police officer, kill him. Kill them all. Kill all of the infidels who persecute you."

1.1.4 Travel of Foreign Terrorist Fighters and Sympathizers Poses an Additional Threat

(U) Mass-casualty attacks in Europe demonstrate that individuals who travel to battlefields in Syria, Iraq, or elsewhere in support of ISIS or other terrorist groups, and eventually return, present a threat to their countries of origin. These individuals are also a potential threat to other countries. On January 7, 2015, for instance, one of the two gunmen who killed 12 journalists at *Charlie Hebdo* magazine in Paris claimed to have acted on behalf of al-Qaeda in Yemen after returning to Europe.[61]

(U) Many of the estimated three dozen suspected ISIS extremists recently arrested in Europe, including at least seven involved in the Paris and Brussels attacks, reportedly had European citizenship when they joined ISIS and then returned as asylum seeking migrants to plot terrorist acts.[62] [63] [64] [65] [66] [67]

(U) These developments raise concerns about ISIS fighters from the United States, Europe, or visa-waiver countries who could face relatively few obstacles to legal or illegal travel to the US. Methods of entering the US would include legal resettlement in Texas as poorly backgrounded refugees or, as a separate issue, the illegal exploitation by special interest alien migrants (SIAs) of established smuggling networks to travel through Latin America to the US-Mexico border.

(U) Texas Residents Traveling to Join Foreign Terrorist Groups

(U) Five Texas cases illustrate the prospect that still more Texas residents have joined or will try to join terrorist groups abroad, raising concerns that some will return with plans to cause harm.[68] [69]

(U) In January 2016, Houston resident and Iraqi-born refugee Omar Faraj Saeed Al-Hardan was indicted for planning to join ISIS and to bomb two Houston malls when his travel plans stalled. Al-Hardan, a legally resettled refugee who was granted legal permanent resident status in August 2011,[70] reportedly began planning to join ISIL in May 2014 and made false statements to federal investigators regarding automatic weapons training he received overseas with ISIS. In addition, Al-Hardan maintained ties to al-Qaeda's Syrian affiliate.[71] In October, he pleaded guilty to providing material support to ISIS.[72]

(U) Mesquite resident Bilal Hamed Abood, an Iraqi-born naturalized US citizen, succeeded in traveling to a rebel group in Syria and returning to the state. The FBI arrested Abood in May 2015 for lying about initial plans to travel to Syria in 2013 to join rebel fighters. At D/FW International Airport, homeland security authorities refused to let Abood board his overseas flight. But a short time later, in April 2013, Abood found his way there by departing through Mexico.[73]

(U) After his September 2013 return, Abood told the FBI that he spent time in Syria with a rebel group not banned under US law, and that he did not support the banned terrorist group ISIS.[74] However, the FBI later learned from a search warrant on Abood's computer that he wanted to "help build the Islamic State of Iraq" and that he had pledged an oath to ISIS leader Abu Bakr al-Baghdadi. The FBI finally arrested Abood for the original lie he told in 2013 at the D/FW airport.

(U) In May 2015, the FBI arrested Spring, Texas, resident Asher Abid Khan after a lengthy investigation during which he traveled as far as Turkey on his way to join ISIS. Khan allegedly was hoping to die a martyr fighting with ISIS but was arrested after he was tricked into returning to Texas by reports that his mother was gravely ill. [75] A Texas associate of Khan's, described as a "Mexican convert," succeeded in joining ISIS in fighting.[76]

(U) The Abood, Khan, and Al-Hardan cases are on the most recent examples involving Texans wanting to join extremists in fighting abroad. Back in June 2014, the FBI arrested Austin-area resident Michael Todd Wolfe for planning to join ISIS and Rahatul Ashikim Khan, who at one point hoped to join al-Shabaab in Somalia.

(U) Of those who succeeded in traveling overseas, several have died in operations, including Moner Abu-Salha, a resident of Florida who was reportedly radicalized and funded in Texas.[77]

(U) We assess that the threat of legal or illegal returns will remain elevated, given the high rate of foreign fighter travel to Syria, which exceeds the rate of travelers who went to Afghanistan, Pakistan, Iraq, Yemen, or Somalia at any point in the last 20 years[78] and the fact that:

- (U) The current conflict in Syria has drawn nearly 40,000 foreign fighters from more than 120 countries, many of whom have joined ISIS.[79] As of April 2016, these included at least 6,900 fighters from Western countries, of whom more than 1,000 have returned to the UK, France, Germany, and Belgium.[80]

- (U) Approximately 250 Americans, including numerous Texas residents, have been involved in various stages of travel to Syria, including those who attempted but did not go, those who went and fought, those who died, and a small number who returned to the US.[81]

(U) US-based Aspiring Foreign Terrorist Fighters Exiting Through Mexico

(U) In recent years, US and Canadian law enforcement have greatly expanded a campaign to detect and interdict Americans seeking to join ISIS and other US-designated terrorist groups abroad. One key tool is the use of the US No-Fly List, which prevents airline travel to or from US territory. Adapting to defeat the No-Fly List, however, at least 13 known aspiring foreign terrorist fighters since 2012 have crossed or planned to cross the US-Mexico border in transit to join foreign terrorist organizations in Iraq, Syria, Somalia and Pakistan. Most of the aspiring fighters knew they were on the No-Fly List and under FBI investigation when they sought to reach conflict zones through Mexico, four of them successfully. Mexico does not collaborate with No-Fly List enforcement to the extent that Canada does. The instances[82] [83] in which aspiring foreign terrorist fighters planned transit through Mexico, as well as analysis of the circumstances surrounding their travel, suggests that use of this tactic presents an opportunity for increasing numbers of aspiring foreign terrorist fighters to evade US interdiction efforts such as the No-Fly List. Among the cases:

- (U) On October 4, 2016, two Milwaukee, Wisconsin men were arrested near San Angelo, Texas on their way to Mexico as part of an alleged plan to join the Islamic State of Iraq and Syria (ISIS), an FBI criminal complaint alleged.[84] Texas DPS troopers, local officers and FBI agents, who had been tracking the two as they traveled, arrested Islamic converts Jason Michael Ludke and Yosvany Pedilla-Conde, a Cuban national, on US Highway 87 in Tom Green County.[85] The arrests occurred on the final leg of a car journey from Milwaukee to El Paso, where the men allegedly hoped to cross to Juarez, Mexico, and acquire fraudulent passports, possibly to fly from Brazil to reach ISIS in Raqqa, Syria, before traveling to Mosul, Iraq.[86] [87]

- (U) In April 2015, seven Minnesota men of Somali descent were arrested in San Diego and Minnesota for conspiring to go to fight with ISIS in Syria, by crossing the California-Mexico border. The men were arrested prior to carrying out the plan.[88] According to a May 2015 federal indictment, the group discussed obtaining false Mexican passports from another friend already in Syria. The plan was to fly from Mexico to Turkey, and then travel into Syria. [89]

- (U) In April 2015, after returning from Syria, Iraqi-born Mesquite, Texas resident Bilal Hamed Abood was arrested for lying to the FBI by claiming that he had not pledged allegiance to ISIS.[90] Two years earlier, in April 2013, Abood crossed the Mexico land border, boarded a Mexican airline to Bogota, Colombia, and made his way to Syria, where he claims to have fought with the Free Syrian Army.[91]

- (U) In October 2013, the US-born extremist Sinh Vinh Ngo Nguyen was arrested while attempting to cross into Mexico from California with airline tickets to Peshawar, Pakistan, where he was to train al-Qaeda fighters.[92] Nguyen, who also went by the name Hasan Abu Omar Ghannoum, had previously traveled to Syria and fought for five months with the al-Qaeda-affiliated al-Nusra Front against the Syrian government. [93]

- (U) In July 2012, Somali-born US citizen Liban Haji Mohamed drove from his home state of Virginia to the Texas-Mexico border, slipping past his FBI surveillance team along the way, and then crossing the border.[94] He flew to Somalia from Mexico to join the terrorist group al-Shabaab, and was later placed on the FBI's Most Wanted terrorist list.[95] [96] The transitional Somali government arrested him in March 2015.

1.2 Domestic Extremism

(U) We are not only concerned about extremists inspired by foreign groups and their online messaging capability. Typically distinct from religiously motivated terrorism, a variety of domestic anti-government groups and movements based in the US often invoke violence-motivating ideologies tied to political or social issues. Lawfully adhering to any political or philosophical ideology is constitutionally protected, and becomes subject to law enforcement interest only when attended by criminal behavior. Domestic ideologies that may occasionally motivate violence in Texas are diverse, ranging on the political spectrum from antigovernment "sovereign citizen" and militia extremists who reject government authority, to violent activism for environmental and animal protection causes. Our concern about the persistence of this threat is underscored by recent events.

- (U) In November 2015, a Houston area man was sentenced to 20 years in prison following convictions for a plot to rob armored cars and then use the proceeds to raise an armed group to attack mosques, police, and government personnel. Robert James Talbot Jr. was arrested following an eight-month undercover FBI investigation of his plans to recruit other anti-government individuals who would blow up government buildings, rob banks, and kill law enforcement officers.[97]

- (U) On November 28, 2014, Texas resident Larry Steven McQuilliams mounted an active-shooter attack in downtown Austin, firing on the federal courthouse, Austin Police Department headquarters, a bank, and the Mexican Consulate General's offices before he was shot dead.[98] McQuilliams, who acted alone and caused no serious injuries, apparently associated himself with the "Phineas Priesthood," an ideology that is sometimes associated with white supremacists, but has rarely inspired such violent acts.[99] The ideology centers on a "leaderless resistance" concept by individuals who claim divine authority to commit murders, bank robberies and assaults against those perceived to be in violation of biblical laws.[100]

- (U) In early October 2014, a corporate sign was vandalized and windows were shot out at the Mary Kay corporate office in Addison. Vandals spray painted "stop animal testing" on the company sign. Gunshots were also fired at the office building, striking and shattering windows near the entryway. An anonymous Internet forum post appeared on an Animal Liberation Front (ALF) site the following day, describing the attack and claiming it was motivated by Mary Kay's decision to continue product sales in China, where mandatory animal testing of imported cosmetics occurs.[101]

(U) After Dallas and Baton Rouge: Threat to Law Enforcement

(U) The July 2016 ambush-style attacks on law enforcement officers in Dallas and Baton Rouge, both perpetrated by lone extremists armed with rifles and handguns, killed or wounded 20 officers in apparent retaliation for perceived wrongful police killings of unarmed criminal suspects.[102] [103] The two attacks further raised concern about the targeting of officers by violent extremists. The Texas and Louisiana ambushes of police appear to have been part of a broader trend. Ambushes of police increased sharply since 2014.[104] [105]

(U) Comprehensive data about the motivations behind all of the police ambushes are not yet widely available, in part because investigations are ongoing, or because suspects have not communicated publicly. However, a review of open source media and court reporting identifies a number of other police ambush attacks since December 2014 where motivations appeared, at least initially, to have involved anti-police sentiment.[106] [107] [108] [109] [110] [111]

- (U) On July 7, 2016, Lakeem Keon Scott of Bristol, Tennessee armed with an assault-style rifle and a handgun opened fire on a hotel and at motorists driving on a Tennessee highway as part of an alleged plot to draw police into an ambush.[112] He killed a newspaper carrier driving in her car, and wounded another person working at the hotel. When police arrived, Scott opened fire at them, seriously wounding an officer before Scott was wounded in the return fire.[113] [114] Investigators alleged that Scott targeted officers in anger over recent events "involving black people and law enforcement officers in other parts of the country."[115] [116]

- (U) In August 2015, a man approached Deputy Sheriff Darren Goforth from behind at a gas station near Houston, shooting him once in the back of his head. Shannon Miles was later charged with firing 15 more shots into the fallen deputy.[117] [118] After the killing, Sheriff Ron Hickman stated that Miles allegedly had been motivated by anger with police for the recent killings of unarmed black suspects.[119] An indictment stated that the motive was "retaliation" for Deputy Goforth's "service and status" as an officer.[120] [121] Miles pled not guilty to capital murder charges, citing mental disorders, but a judge ruled that Miles is mentally competent.[122]

- (U) In December 2014, an assailant ambushed two New York City police officers while they sat in their parked patrol car in Brooklyn, killing them "execution-style."[123] The assailant, Ismaaiyl Brinsley, fled and later died of a self-inflicted gunshot. Brinsley had a lengthy criminal record, including 19 arrests. He vowed in a social media post to put "wings on pigs." Some reports linked Brinsley to the Black Guerilla Family, a radical prison gang that had called for attacks on police earlier that month and has continued to plot attacks.[124]

- (U) In November 2014, authorities arrested and convicted two men for plotting to blow up a police station and the St. Louis Gateway Arch, and murder the police chief and a county prosecutor in Ferguson, Missouri.[125] Olajuwon "Ali" Davis and Orlando Baldwin fraudulently acquired firearms and began conspiring with an undercover FBI informant to build an explosive device.[126] In June 2015, Davis and Baldwin were each sentenced to 84 months in prison.[127] Investigators stated that both men had been involved in anti-police protests.[128] [129]

(U) In response to the threat, some law enforcement agencies have implemented paired patrols and increased security around police headquarters and government buildings, acquiring armored vehicles and posting officers armed with rifles outside station entrances.

2. Crime

(U) Crime threatens the public safety and liberty of all Texans in some way. The Texas Department of Public Safety's Uniform Crime Reporting program data for 2015 shows a 4.7 percent decrease of the major crime rate in Texas from 2014. This is positive news overall for the safety and welfare of our citizens. Conversely, violent crimes increased for the second year. The program captures seven index crimes: homicide, rape, robbery, aggravated assault, burglary, larceny, and vehicle theft.[130]

(U) The number of violent crimes reported in Texas increased 3.7 percent from 2014 to 2015. For example, 1,314 murders were reported in 2015, as compared to 1,187 for 2014, a 10.7 percent increase. The index crime data does not currently account for other crimes typically committed by criminal organizations that also impact the security of Texas communities, such as human trafficking, drug trafficking, kidnapping, extortion, money laundering, public corruption, and the exploitation of juveniles for criminal activity. This section assesses some of those criminal threats.[131]

2.1 Human Trafficking

(U) Individual criminals and criminal organizations – including Mexican cartels and transnational gangs – engage in a wide range of illicit activity in Texas. Among the vilest of their crimes is the exploitation and trafficking of children and other vulnerable victims. Such crimes are also carried out and enabled by human smugglers, prostitution rings and buyers of commercial sex, manufacturers and viewers of child pornography, and sexual predators. Regardless of who perpetrates them or why, we regard this criminal activity as especially heinous, as it subjects children and vulnerable victims to violence, extortion, forced labor, sexual assault, and prostitution.

(U) Human trafficking involves the transportation, enticement, recruitment, harboring, providing, or otherwise obtaining any person by any means for labor or services for the purpose of involuntary servitude, slavery, or forced commercial sex acts. In Texas, criminal organizations and individual criminals target male and female victims of different ages, nationalities, and socioeconomic classes.

(U) Estimates vary for the number of trafficking victims in Texas or the United States, and the available data is not comprehensive. These data limitations are due to several challenges, such as the under-reporting of trafficking to law enforcement, definitional differences or variations among agencies, and the use of varying criminal charges for crimes that are not trafficking per se, but initially involve trafficking.[132] However, during the 2015 Texas Legislative Session, House Bill 2455 was passed, ordering all agencies conducting investigations of this nature "to promote uniformity in the collection and reporting of information relating to family violence, sexual assault, stalking, and human trafficking."

2.1.1 Sex Trafficking and Compelling Prostitution

(U) Sex trafficking and compelling prostitution is defined as forcing victims into prostitution or commercial sex for the benefit of the trafficker and against the victims' will; although force, fraud, or coercion do not have to be proven in the case of minors involved in either labor or commercial sex trafficking. Sex trafficking continues to be a problem around the world, including in Texas. It is the fastest-growing business of organized crime and the third-largest criminal enterprise in the world.[133] Sex trafficking involves domestic and international victims, males and females, and children and adults.

(U) Traffickers are commonly referred to as "pimps." They are typically in charge of luring, marketing, and transporting their victims to and from their meetings with customers.[134] These individuals collaborate

to recruit, control, and advertise their victims, and then keep all revenue, in addition to using coercion, physically assault, and false affection to lure victims.

(U) Pimps and trafficking organizations use a variety of methods and means to target and recruit victims and to advertise the victims' illegal sexual "services" to customers. Many traffickers rotate victims through various cities and locations and operate out of hotels or with little infrastructure.

(U) Sex traffickers in Texas target juvenile runaways, illegal aliens, and other vulnerable victims using force, fraud, and coercion to compel them into the sex trade. Often, victims are manipulated and controlled by traffickers to remain with them due to their emotional or financial dependency on the trafficker for food or housing, and traffickers may also restrict the victims' access to communication with friends and family. Many traffickers physically and sexually assault their victims and threaten family members to deter victim escapes. These cases demonstrate some of the abuses:

- (U) In February 2016, four defendants in Houston were sentenced to federal prison for trafficking women and girls under 18. One woman, who is a legal permanent resident, was convicted of sex trafficking of a minor and harboring illegal aliens. A female legal permanent resident, a female naturalized US citizen, and a Cuban citizen pled guilty to engaging in sex trafficking of minors. From February 2012, the four defendants ran apartment brothels in which the victims were instructed to charge $40 per 15 minutes of commercial sex. The defendants knew their victims were illegal aliens in the US.[135]

- (U) In December 2014, an adult male, an adult female, and a 14-year-old female were arrested for prostitution at a motel in Shreveport, Louisiana. The juvenile was a Texas runaway who traveled from Dallas with the male and female to engage in prostitution. The two adults were charged with human trafficking and marijuana possession.[136]

(U) Traffickers seek out potential customers in classified Internet advertisements and on social networking websites.[137] In other cases, trafficking victims are forced to seek out customers on the street, or use front businesses – such as bars, strip clubs, or massage parlors – to operate. For example, in May 2016, a man was sentenced to 100 months in federal prison for trafficking minors. From May 2011 to May 2012, the FBI and ICE alleged, the man used the Internet to recruit and promote three children for commercial sex in El Paso, Midland, Odessa, San Antonio, and Killeen.[138]

(U) Sex traffickers routinely transport victims among multiple cities to expose them to new markets. This tactic makes law enforcement detection and interdiction more difficult, but can enable higher penalties for interstate trafficking. Large special events that attract large numbers of visitors to a city can prompt traffickers to travel there with their victims. From June to August 2015, the Texas Department of Public Safety investigated a man and woman from Flint, Michigan accused of trafficking girls by posting online "escort" advertisements. The defendants trafficked the minors in Austin and other Texas cities, as well as in Flint and Detroit. In May 2016, a federal jury in Austin found both defendants guilty of sex trafficking of a minor, and of interstate transportation of a minor with the intent to engage in prostitution.[139]

(U) Sex trafficking operations have the potential to generate large and renewable profits, and some criminals reportedly consider sex trafficking and compelling prostitution to be more lucrative and lower risk than other criminal activity. Each organization or trafficker charges a different fee based on various factors including the sexual acts, length of time, location, and any special requests.

(U) We have limited information regarding the extent to which Mexican cartels are directly involved in sex trafficking operations in Texas. But because trafficking operations promise high profits, some state-based transnational gangs reportedly consider sex trafficking as a preferred, low-risk alternative to other

criminal activities such as drug trafficking, robbery, and theft.[140] Some Texas gangs and others elsewhere in the United States conduct sex trafficking with other kinds of criminal operations. Also, individual gang members have been known to work independent of gang leadership endorsement.

(U) Houston Sex Trafficking and Smuggling Enterprise

(U) In January 2016, a 68-year-old Houston woman was sentenced to life in federal prison for operating a 14-member sex trafficking ring over more than a dozen years, harboring illegal aliens and committing money laundering operations along the way. The ring generated more than $1.6 million over just one 19-month period by forcing women and girls to commit prostitution on an upper floor of a local cantina.

(U) Law enforcement rescued 12 young female victims, some as young as 14. All of them testified at trial that pimps recruited them in their home countries by convincing them that they were in love, then brought them illegally into the United States and forced them into prostitution. Victims and their families testified that they were threatened.

(U) All 13 co-defendants pled guilty to their respective roles in the conspiracy, with many admitting to working for the Houston cantina Las Palmas II. All the defendants knew that the cantina concealed, harbored, and shielded illegal aliens. Other co-defendants acknowledged that their roles involved investing proceeds from the enterprise into Houston-area real estate properties.

(U) Investigators discovered 15 real estate assets valued at $2.5 million, all of which will be seized by the federal government and used for restitution for the victims. The three-year investigation was a joint effort conducted by members of the Human Trafficking Rescue Alliance (HTRA), including the FBI, ICE Homeland Security Investigations, Harris County Sheriff's Office, IRS, TABC, Department of State, Texas DPS, and Houston Police Department.

2.1.2 Labor Trafficking

(U) The Texas Penal Code defines forced labor as "labor or services, other than labor or services that constitute sexual conduct … performed or provided by another person and obtained through an actor's use of force, fraud, or coercion."[141] Compared to other kinds of trafficking, limited reporting on labor trafficking in Texas is available. But the crime does occur in Texas. Forced labor victims who work behind closed doors at restaurants or other businesses can be largely invisible to the public and law enforcement, impeding the identification and detection of this crime. Also, victims can be reluctant to report their circumstances due to their immigration status and lack of awareness of labor laws.

(U) Labor traffickers often recruit, transport, and employ legal and illegal immigrants who they bring into the United States for the purpose of profiting on their forced labor and indentured servitude. Victims often come from developing countries around the world, but can include US citizens. Texas' geography also increases its vulnerability to labor trafficking: it has large agricultural and travel industries, and legal and illegal foreign travel through airports, seaports, land ports of entry.[142]

(U) Labor traffickers in Texas have reportedly demanded that their victims work as long as 12 hours a day, 6-7 days per week, with either less than fair wages or none at all. In some cases, victims are kept in locked homes, brutally beaten, and forced to consume drugs that facilitate longer working hours.

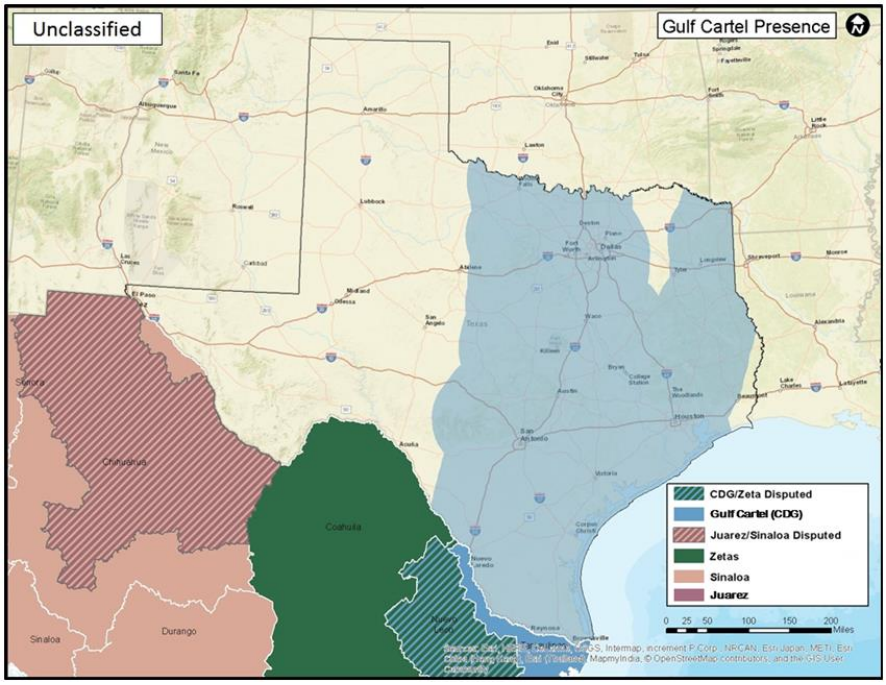
(U) In February 2016, a couple in Houston was sentenced to federal prison for operating an "employment agency" that placed illegal aliens as food service workers in Chinese/Asian restaurants.[143] Victims were compelled to work 12-hour days, six days a week, and were not permitted tips, overtime pay, insurance, food safety training or health examinations. They were forced to live in unfavorable conditions. Eighteen workers, for example, were housed in a single 2,000-square-foot house. In January 2014, law enforcement arrested 32 individuals for a forced labor scheme in Beaumont, and charged them with conspiracies to transport, harbor, and encourage and induce aliens to live in the US.[144]

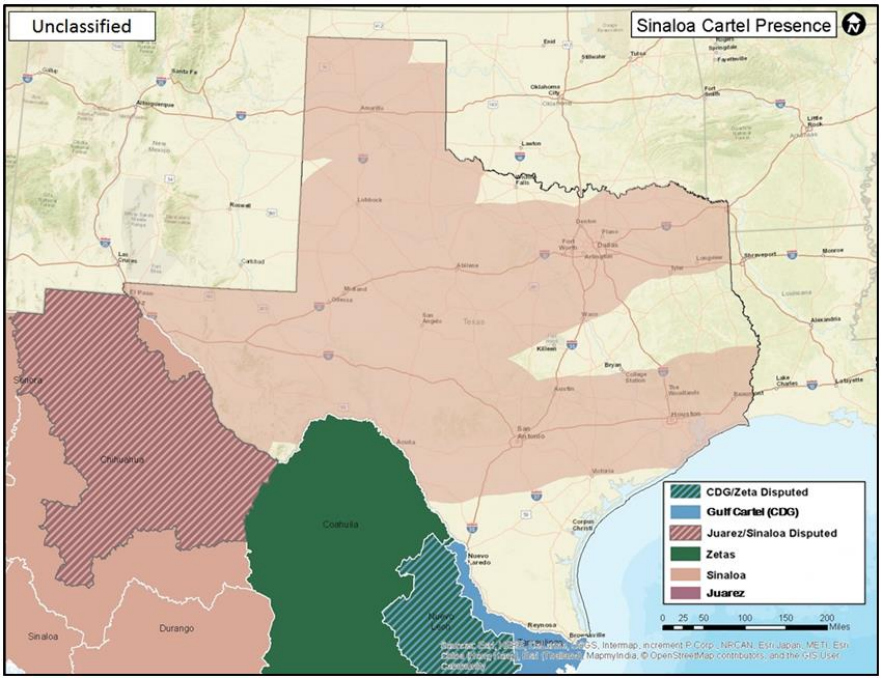
2.2 Mexican Cartels

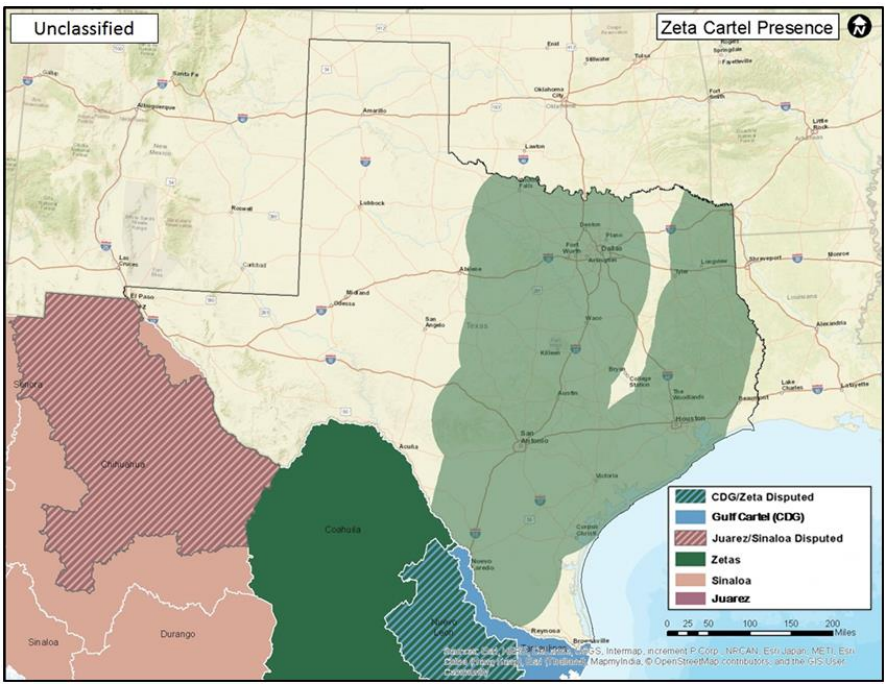
(U) Mexican cartels constitute the greatest organized crime threat to Texas. These powerful and ruthless criminal organizations use military and terrorist tactics to battle each other and the government of Mexico for control over the lucrative US drug and human smuggling markets. They dominate the wholesale trafficking of illegal drugs along the Texas-Mexico border, producing or smuggling most of the illegal drugs to the US. The cartels also engage in other criminal activities beyond drug smuggling, including profiting from human smuggling, weapons and ammunition smuggling, extortion, kidnapping for ransom and robbery.

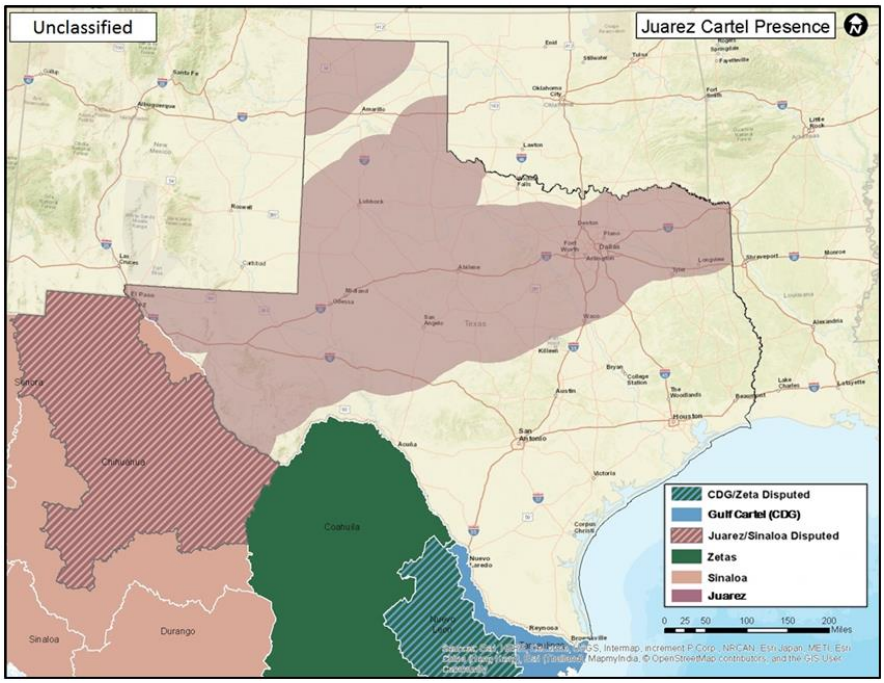
(U) All eight of the major cartels operate in the state, moving drugs and people into the US, and transporting cash, weapons, and stolen vehicles back to Mexico. These include the Gulf Cartel (CDG), Los Zetas, Juarez Cartel, Sinaloa Cartel, Knights Templar, La Familia Michoacana, Cartel Jalisco Nueva Generacion and the Beltran Leyva Organization. Of these, the Gulf Cartel, Los Zetas, the Sinaloa Cartel, and the Juarez Cartel have the most extensive presence and influence throughout Texas.[145] The following maps demonstrate areas known, through cases or intelligence sources, to have a presence or be used by cartels for transportation. The threat from Mexican cartels is particularly high due to their wide range of criminal activity in Mexico and in Texas. Cartel members and associates are involved in the cross-border smuggling of people, weapons, drugs, and currency. Their operations are either run directly by cartel members, or indirectly through affiliated criminal organizations that pay fees to transit across cartel territory.

(U) Approximate Areas of Operation of the Top Four Mexican Cartels Operating in Texas




Unclassified
Sinaloa Cartel Presence
CDG/Zeta Disputed
Gulf Cartel (CDG)
Juarez/Sinaloa Disputed
Zetas
Sinaloa
Juarez
0 25 50 100 150 200
Miles
Chihuahua
Coahuila
Durango
Sinaloa


Unclassified
Zeta Cartel Presence
CDG/Zeta Disputed
Gulf Cartel (CDG)
Juarez/Sinaloa Disputed
Zetas
Sinaloa
Juarez
0 25 50 100 150 200
Miles
Chihuahua
Coahuila
Durango
Sinaloa

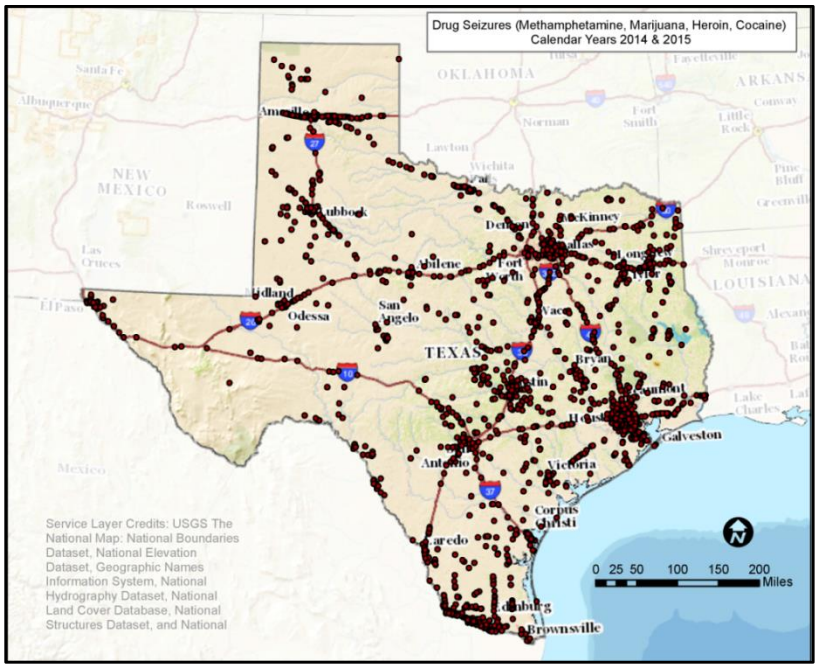


(U) Cartel operatives and associates have engaged in home invasions and other acts of violence in Texas. These crimes are often aimed at recovering lost drug loads, intimidating or silencing rivals and witnesses, and retaliating against enemies. For example, in May 2016, two Mexican citizens were convicted of conspiracy to commit murder for hire and interstate stalking, while a third pled guilty before trial, for their roles in the 2013 murder of a Southlake, Texas attorney they shot and killed in his SUV. The victim was also a Mexican national and reportedly a former attorney for a leader of the Gulf Cartel. From 2011 through 2013, the three defendants traveled from Mexico to Southlake with the intent to kill the victim. They purchased and placed surveillance cameras around the victim's neighborhood to track him and his family, in addition to placing tracking devices on their vehicles. While in the area, the defendants continually bought and rented new vehicles in order to avoid detection.[146]

2.2.1 Drug Trafficking

(U) Mexican cartels directly supply illicit drugs to cities throughout the US and rely on US-based gangs to further distribute drugs. Mexican drug traffickers have increased production of heroin significantly and have probably increased methamphetamine production for the US market, according to the Worldwide Threat Assessment of the US Intelligence Community.[147]

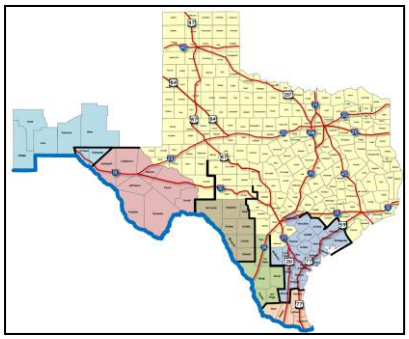
(U) Marijuana remains the most commonly used and most widely available illicit drug in the US. Marijuana continues to be smuggled from Mexico in large volumes, even though domestic production has increased.[148] The majority of cocaine available in the US is produced in South America and smuggled across the Southwest Border. Despite the overall reported decrease in supply, cocaine remains widely available in US markets.[149] Mexico-produced methamphetamine also is available in the US due to sustained production in Mexico. Large shipments are regularly seized at the Southwest Border. Heroin availability is increasing throughout the country, with National Seizure System data showing an 80 percent increase in seizures in the past five years.[150] Seizures at the Southwest Border are also rising as Mexican cartels increase heroin production and transportation.



(U) Texas Department of Public Safety Highway Patrol seizures

(U) The table below shows the value of drugs seized in the 54 Operation Border Star counties with values from the Office of National Drug Control Policy (ONDCP).[151]

Border Region Drug Seizures 2006 2015		
Drug	**Amount Seized (lbs.)**	**ONDCP 2012Value[152]**
Marijuana	12,249,567	$74,342,622,123
Cocaine	107,497	$6,608,808,063
Heroin	5,263	$677,142,843
Meth	22,885	$1,993,672,545
Total	**12,385,212**	**$83,622,245,574**



(U) The cartels take advantage of the large volume of legitimate travel and trade between Texas and Mexico to camouflage their criminal activities. They use many kinds of vehicles, including stolen commercial vehicles, as well as legally registered commercial vehicles, for transporting contraband. And as drugs flow into the United States, cash flows out, with Mexican cartels laundering billions of dollars a year in associated proceeds.

(U) Gang members associated with the Mexican cartels in the Rio Grande Valley use various tactics to evade law enforcement. For example, the Mexican cartels have deployed a substantial number of scouts to conduct around-the-clock surveillance of law enforcement at hotels, airports, restaurants, observation posts and on the river. More concerning is their willingness to use violence against law enforcement officers, as well as to engage in other evasion tactics – such as the deployment of spiked, tire-puncturing caltrops on public roads – which place officers and the public at risk, as in these instances:

- (U) In March 2016, the Texas Highway Patrol, US Border Patrol, and Escobares (Texas) Police Department were pursuing a vehicle transporting narcotics near Rio Grande City, Texas. During the pursuit, the suspect rammed the Escobares Police Department vehicle in an attempt to evade arrest. The driver was arrested, and the narcotics in the vehicle were seized.[153]

- (U) In October 2015, US Border Patrol agents followed a vehicle suspected of containing narcotics near the Rio Grande River in Brownsville, Texas when a passenger inside the vehicle threw caltrops onto the roadway in an attempt to disable the Border Patrol vehicle. The suspect vehicle was later found abandoned with several hundred pounds of marijuana.[154]

- (U) In July 2014, in Anzalduas, Texas, eight to 12 subjects from the Mexican side of the river threw rocks at a DPS shallow water boat that had been conducting deterrence operations along the Rio Grande River. One subject on a Jet Ski rammed the DPS boat as its crew was attempting to arrest another suspect in the river. Both subjects returned to Mexico, abandoning the Jet Ski.[155]

2.3 Human Smuggling

(U) We judge that nearly all illegal aliens who illegally enter the United States make use of alien smuggling organizations (ASOs). These criminal organizations guide groups of illegal aliens across the border and through the Ports of Entry and, in many cases, continue to move them through a series of stash houses in the United States en route to a destination beyond the immediate border.

(U) Human smuggling along the US-Mexico border involves aliens voluntarily hiring ASOs to illegally transport them into or through the United States. This includes bringing illegal aliens into the country, as well as the unlawful transportation and harboring of aliens already in the United States. Although we refer to them as ASOs, many transnational criminal organizations involved in human smuggling also engage in other cross-border smuggling crimes, some of them involving violence.[156]

(U) After smuggling groups of illegal aliens across the border, ASOs often move them through a series of human stash houses, which may occasionally be abandoned homes, ranch dwellings, business locations, storage sheds, warehouses, mobile homes, hotels, or apartments along routes through or to different cities. The length of stay in a stash house may range from a few hours to several weeks. Some stash houses are used by multiple ASOs.

(U) Mexican Cartel Control of Human Smuggling Along the Border

(U) We judge that Mexican cartels control, facilitate, or benefit from nearly all human smuggling activity along the U.S.-Mexico border. The leaders and members of Los Zetas, the Gulf Cartel, the Juarez Cartel, and the Sinaloa Cartel command and control human smuggling operations or employ cartel operatives to manage or oversee human smuggling operations in their territory along the U.S.-Mexico border. In some cases, cartel members and associates participate in human smuggling operations, possibly independently of the orders or oversight of cartel leaders. Some cartel-ASO connections are indirect and are limited to ASOs being required to pay a cartel for operating in its territory.

(U) However, even given such indirect relationships, the cartels facilitate or benefit from the ASOs' operations, and, in most cases, the cartels set rules on whether, how, or where ASOs may operate. We assess that the cartels have profited from the increase in illegal crossings in 2014 and 2015.

2.3.1 Apprehensions Remain High and Concentrated in the RGV

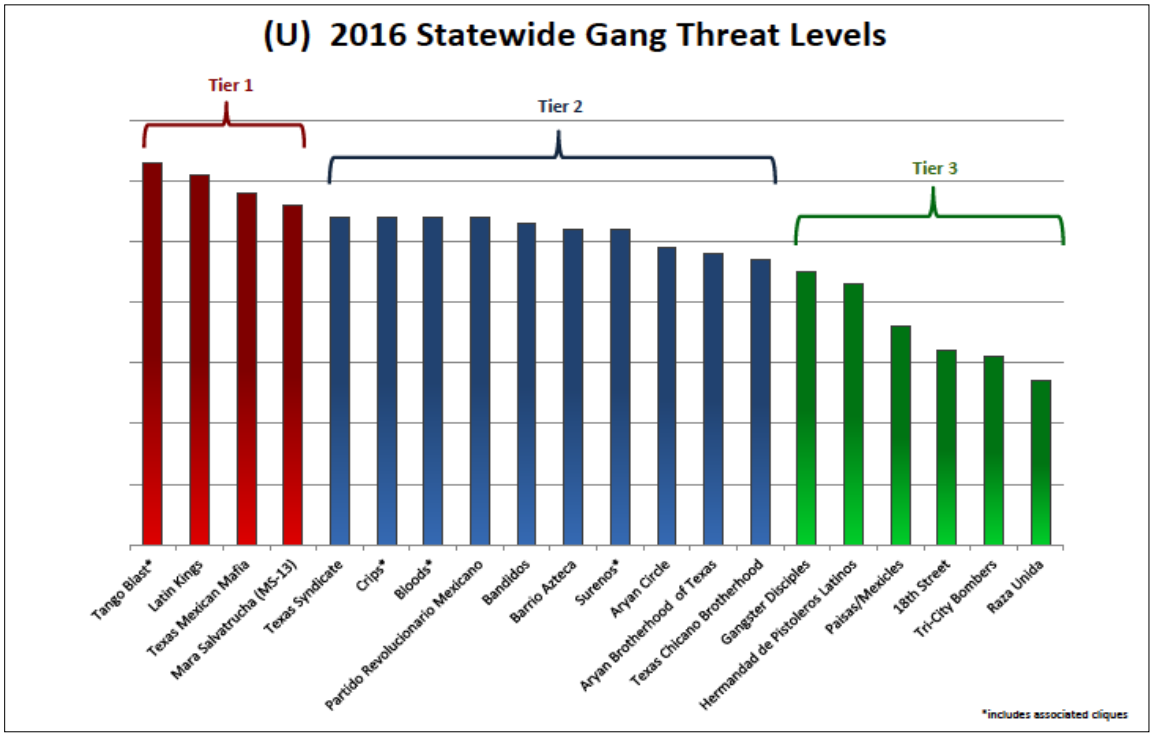
(U) The US-Mexico border has long been vulnerable to illegal entry between ports of entry. After trending downward for several years from a peak in FY2000, the number of illegal alien apprehensions along the border increased each year since FY2011, reaching 479,371 in FY2014, which represents the highest number since FY2009. Total apprehensions considerably decreased in 2015.[157]

(U) Although apprehensions occur along the entire Southwest Border, they are currently most concentrated in South Texas, including the Rio Grande Valley sector of Texas. Following a peak in FY2014, the number of total apprehensions in the Rio Grande Valley has declined but remains high compared with previous years.

2.4 Gangs

(U) Gangs continue to represent a significant public safety threat to Texas, and their propensity for violence and other criminal activities remains constant. The Joint Crime Information Center uses a risk assessment matrix to compare and evaluate the threat posed by individual gangs at a statewide level. A matrix consisting of multiple factors is used in determining each gang's threat potential. The factors are rated using a weighted, point-based system to achieve a composite score. This score provides a measurement of the overall threat level of each gang. Gangs with the highest score are deemed the most significant and are classified as Tier 1, with other significant gangs classified as Tier 2 and Tier 3. Considering that thousands of gangs have been identified in Texas, this threat assessment matrix is an essential tool in prioritizing which gangs pose the greatest threat on a statewide scale.

(U) The Tier 1 gangs in Texas for 2016 are Tango Blast and Tango cliques, Latin Kings, Texas Mexican Mafia, and Mara Salvatrucha (MS-13). These groups pose the greatest gang threat to Texas due to their relationships with Mexican cartels, high levels of transnational criminal activity, high levels of violence, and overall statewide presence.

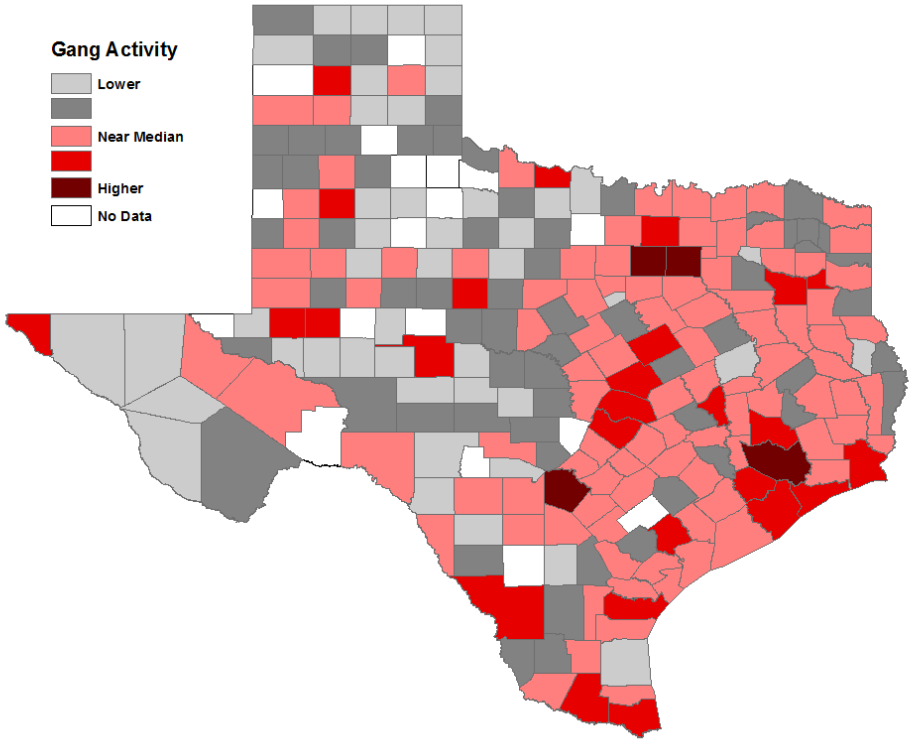


(U) Gang activity remains widespread throughout all areas of Texas. While the greatest concentrations of gang activity tend to be in the larger metropolitan areas, gang members are also present in the surrounding suburban and rural areas. Gang activity is especially prevalent in the counties adjacent to Mexico and along key smuggling corridors, since many Texas-based gangs are involved in cross-border smuggling and trafficking. Many transnational gangs operating in Texas, such as Barrio Azteca and MS-13, engage in criminal activity in Mexico and elsewhere.

(U) Law enforcement agencies in Texas have identified thousands of individual gangs statewide, though it is unknown how many are active. These gangs range from small groups with limited geographic reach, to large organizations with thousands of members throughout Texas, the United States and Mexico.

(U) Gangs in Texas remain active in both human smuggling and human trafficking operations. Gang members associated with human smuggling maintain direct relationships with alien smuggling organizations (ASOs) and Mexican cartels, which were all involved in and profited from the 2014 influx of Central Americans crossing the border in the Rio Grande Valley. Gang members involved in human trafficking, including commercial sex trafficking and compelling prostitution of adults and minors, exploit their victims through force, fraud or coercion, including recruiting and grooming them with false promises of affection, employment, or a better life.

(U) Mexican cartels regularly use Texas gangs for the purposes of illicit cross-border smuggling. Members of Tier 1, Tier 2, and other gangs are sometimes recruited and tasked by cartels to carry out acts of violence in both Texas and Mexico. The relationships between certain gangs and cartels fluctuate based on cartel structures and cell alignments, gang alignment with specific cartels, threats or coercion, and familial ties.



(U) Increasing Threat from MS-13 in Texas

(U) Mara Salvatrucha (MS-13), whose members are known for highly violent crimes such as brutal murders and dismemberments, emerged as a top-tier gang threat in Texas in 2015. The increase of illegal alien gang members crossing the border into Texas among unaccompanied minors the previous year, along with reports of extremely violent murders committed by its members in the Houston area, positioned the gang as one of the state's most significant gang threats.

(U) Although significant numbers of MS-13 members have been captured along the border, it is likely that many more have successfully crossed into Texas and remain hidden from law enforcement, most likely in cities with large Central American communities. Law enforcement agencies in Houston, for instance, report the highest number of identified MS-13 members in the state, followed by Dallas.[158] Several recent crimes in Texas illustrate the criminal threat associated with MS-13:

- (U) In April 2016, two males from El Salvador were each sentenced to 35 years in federal prison for their roles in the murder of a 16-year-old whose body was discovered in the Sam Houston National Forest north of Houston. The men admitted to murdering the victim with a baseball bat and a machete, nearly decapitating him and mutilating his body on gang orders.[159]

- (U) In June 2016, the alleged leader of a Houston area MS-13 clique was sentenced to 99 years for the murder of a 14-year-old student. The 23-year-old man ordered and participated in murdering the teen with a machete along with three other gang members, for the teen's refusal to kill his own cousin in a gang ritual.[160]

2.5 Criminal Arrests of Illegal Aliens in Texas

(U) According to DHS status indicators, over 207,000 criminal aliens have been booked into local Texas jails between June 1, 2011 and November 30, 2016. During their criminal careers, these criminal aliens were charged with more than 553,752 criminal offenses. Those arrests include 1,118 homicide charges; 65,965 assault charges; 16,186 burglary charges; 65,506 drug charges; 674 kidnapping charges; 39,354 theft charges; 43,309 obstructing police charges; 3,646 robbery charges; 5,827 sexual assault charges; and 8,283 weapons charges. Of the total criminal aliens arrested in that timeframe, over 138,000 or 66% were identified by DHS status as being in the US illegally at the time of their last arrest.

(U) According to DPS criminal history records, those criminal charges have thus far resulted in over 248,000 convictions including 462 homicide convictions; 24,680 assault convictions; 7,859 burglary convictions; 32,457 drug convictions; 226 kidnapping convictions; 17,833 theft convictions; 21,280 obstructing police convictions; 1,841 robbery convictions; 2,644 sexual assault convictions; and 3,456 weapons convictions. Of the convictions associated with criminal alien arrests, over 165,000 or 66% are associated with aliens who were identified by DHS status as being in the US illegally at the time of their last arrest.[161]

(U) Threats to Schools

(U) The most precious resource in Texas is our children. In 2013-2014, there were 5.2 million children in Texas' 8,571 public schools, and an additional 1.6 million students at over 250 campuses of higher education. Some students are transported daily on 40,612 buses, including 8,792 special-needs buses.

(U) Schools represent potential soft targets that are vulnerable to a range of threats. School shootings have been a topic of concern for law enforcement and homeland security for many years, as terrorists, criminals, and the mentally unstable have attacked schools in Texas, throughout the United States, and around the world, such as:

- (U) On June 1, 2016: An Indian-born Ph.D. student killed his former associate professor at the University of California, Los Angeles.[162] At the time of the shooting, hundreds of students were attending classes in the Engineering IV building where the shooting took place. The gunman ultimately committed suicide prior to authorities apprehending him.[163] A "kill list" that outlined other targets at the university was recovered after the crime.[164]

- (U) On October 1, 2015: A man armed with several handguns opened fire in a classroom on the campus of Umpqua Community College near Roseburg, Oregon, killing nine people and wounding several others.

- (U) On April 2, 2015: Men armed with firearms and explosives attacked the campus of Garissa University College in Kenya, taking hostages and ultimately killing 147 people. The Somali terrorist group Al-Shabaab claimed responsibility for the attack.[165]

- (U) On December 16, 2014: Six Taliban gunmen entered the Army Public School and Degree College in Peshawar, Pakistan, and stormed classrooms, shooting and killing students, many of whom were young children. Police arrived and exchanged gunfire with the gunmen, ultimately killing them. This tragic incident left at least 140 students dead, 80 in grades one through ten.[166]

2.6 Public Corruption

(U) Public servants who engage in illegal activity or conspire with criminal organizations not only contribute to the furtherance of crime, they betray the public trust. In cases of law enforcement corruption, officers undermine the criminal justice system and turn a blind eye to the activities of criminal organizations. This form of corruption is especially of concern along the Texas-Mexico border, where corrupt public officials who permit traffickers to operate with impunity potentially allow drugs, people, weapons, and other unknown threats to enter the country.

(U) In particular, Mexican cartels are adept at corrupting law enforcement officers in Mexico, and they also seek to corrupt public officials in the United States. Since October 1, 2004, more than 140 Customs and Border Protection employees have been arrested or indicted for acts of corruption that justify persistent concern, such as drug and alien smuggling, money laundering, and conspiracy. For example:

- (U) In May 2016, a Border Patrol agent, an Edinburg police officer, and a former Houston police officer were among 15 individuals charged in a cocaine trafficking conspiracy as a result of the four-year "Operation Blue Shame" investigation. The defendants face charges of conspiracy to possess with intent to distribute cocaine, and other possession charges.[167]

- (U) In February 2016, a Border Patrol agent was arraigned for his alleged connection to a cartel-related murder in Edinburg, Texas. The victim's body was found decapitated and floating in the Laguna Madre, near South Padre Island, in March 2015. The man was murdered because he intended to go to the authorities about a Gulf Cartel-linked trafficking organization.[168]

- (U) In October 2015, federal authorities announced the arrest of a former DPS employee and one other subject in connection with a scheme to provide driver licenses to illegal aliens. According to the indictment, the defendants conspired from May 2013 to July 2015 to transfer driver licenses, knowing that such documents were produced without lawful authority.

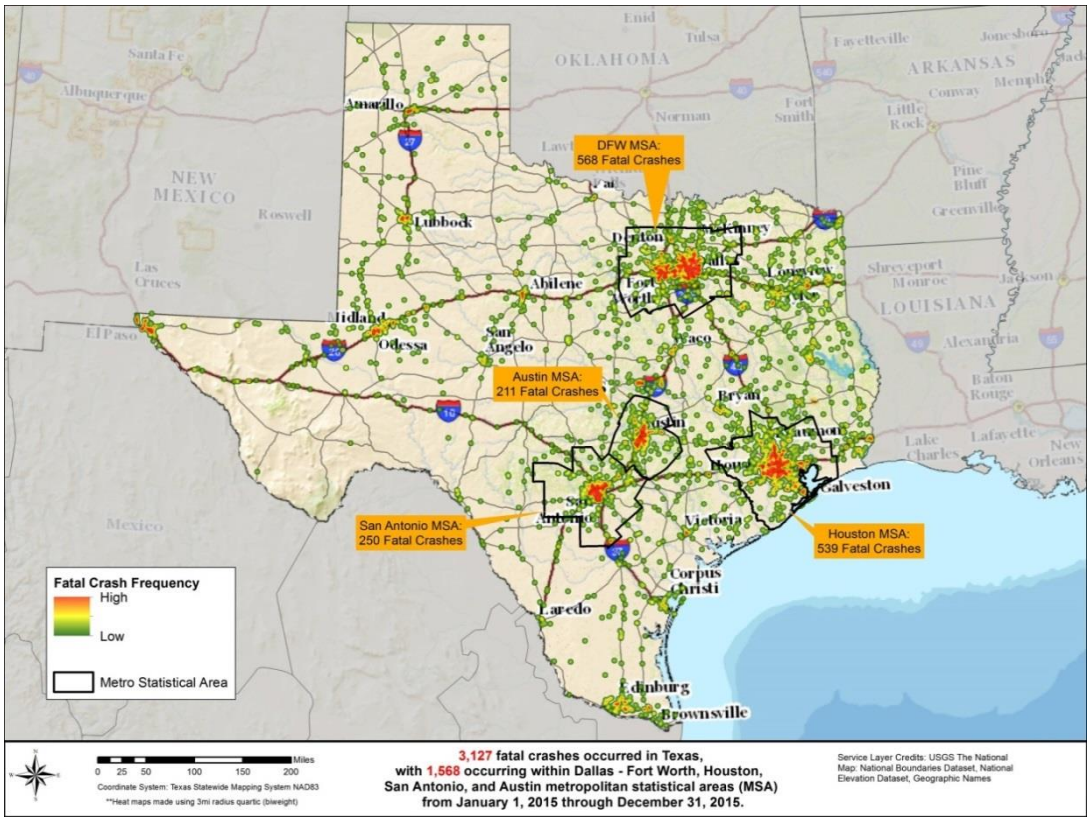
- (U) In November 2014, a Border Patrol agent pled guilty to harboring illegal aliens at a residence in Laredo, Texas. For approximately one year, the agent was aware of the five illegal aliens who were living at the house, and of their illegal presence in the United States. He also admitted knowing that two of the individuals had previously been deported.[169]

- (U) In May 2014, former Hidalgo County Sheriff's Office deputy Robert Ricardo Maldonado pled guilty to money laundering. From 2001 to November 2013, he transported currency derived from the distribution of narcotics to Chicago, Birmingham, and Detroit. He had been paid a percentage of the transported currency, and had bought various assets and properties.[170]

- (U) In April 2014, Jonathan Trevino, a Mission, Texas Police Department officer was sentenced to 17 years in prison for an elaborate drug conspiracy that took place while he was participating in the narcotics task force known as the Panama Drug Task Force Unit. Also sentenced was his partner and friend, Alexis Espinoza, a former Mission Police Department officer, as were 10 other officers.

- (U) In March 2014, in Hidalgo County, Texas, former Hidalgo County Sheriff Lupe Trevino was arrested and convicted on federal money laundering charges for accepting campaign contributions from a drug trafficker. Trevino's chief of staff was also convicted in relation to the crime, while former Hidalgo County Sheriff's Office Commander Jose Padilla was arrested for accepting bribes in exchange for confidential law enforcement information.

3. Motor Vehicle Crashes



(U) Ensuring the safe and efficient flow of people and commerce on Texas' 313,596 miles of roadways is a critical responsibility shared by law enforcement and other government agencies across the state.[171] More than 17,357,632 drivers, including 743,964 teenage drivers, are licensed to drive these roads.[172] More than 24 million vehicles are registered, including 19,521 buses and 268,868 commercial motor vehicles (CMVs).[173] Each year, motor vehicle crashes account for significant loss of life and economic costs across the state. Approximately 3,520 motor vehicle traffic fatalities were reported in 2015 and 3,536 in 2014.

(U) Large truck traffic in Texas has grown substantially over the past 20 years, due to commercial and residential growth, oil and gas drilling, and the expansion of commerce with Mexico.[174]

(U) Texas leads the nation in fatal crashes involving CMVs.[175] Crashes involving these larger and heavier vehicles have serious consequences, making them more likely to result in deaths. In 2015, CMV crashes resulted in 599 fatalities. The top contributing factor in CMV-related crashes was the CMV driver's failure to control speed. From January 1 to April 30, 2016, CMV-related crashes resulted in 153 fatalities.[176]

(U) CMV-related crashes pose potential dangers to individuals beyond those who are directly involved. The frequent transportation of hazardous, toxic, and even radioactive materials using CMVs, for instance, poses a potential threat to both populated and unpopulated areas of the state.

(U) Impaired Driving Fatal Crashes in Texas

(U) In 2015, there were 956 fatalities resulting from crashes that involved drunken driving, a decrease from 1,086 in 2014. Another 239 persons died between January 1 and April 30, 2016. Deaths from driving under the influence of drugs also signaled a significant ongoing problem. From January 1 to April 30, 2016, there were 100 fatalities in crashes involving someone driving under the influence of a drug,[177] compared to a yearlong total of 611 in 2015, and 614 in 2014.

(U) Certain high-population areas consistently report the most drunken driving deaths. In 2015, Harris County reported the highest number of fatal crashes in Texas that involved a person under the influence of alcohol, with 104, followed Dallas County with 77, and Bexar County with 62. From January 1 to April 30, 2016, Harris County reported the highest number, with 33 fatal crashes. Dallas County reported 23, and Bexar County reported 12.[178]

(U) As for driving under the influence of drugs from January 1 to April 30, 2016, Dallas County led with 59 fatal crashes, followed by Harris County with 50, and Bexar County with 31. From January 1 to April 30, 2016, Dallas County reported 17 fatal crashes involving driving under the influence of drugs, with Harris County reporting nine, and Montgomery County (to its north) eight.[179]

(U) Under Texas law, driving under the influence of alcohol or drugs is a criminal offense that can have serious legal consequences. A person's first two driving while intoxicated (DWI) convictions are categorized as misdemeanors, while the third offense is a felony of the third degree.[180] Texas law provides zero tolerance for minors who drive under the influence, which can result in a license suspension, fine, community service, and alcohol-awareness classes.[181]

(U) Driving while distracted, especially while texting or otherwise using a cell phone, poses a recognized public safety hazard that has resulted in deaths and injuries across Texas. Each day in the United States, approximately nine people are killed and more than 1,150 people are injured as a result of distracted driving.[182] One in five Texas vehicle crashes involves distracted driving.[183] Texas crashes involving distracted drivers increased from 101,005 crashes in 2014 to 103,561 in 2015. These crashes are highest among young adults ages 20 to 29, followed by teenagers 19 and under.[184] In 2015, a total of 474 fatalities in Texas involved distracted drivers. Bexar County had the highest number of fatalities with 56. Travis County accounted for 28 fatalities and Dallas County had 27. From January 1 to April 30, 2016, there were 33,675 crashes and 133 fatalities involving a distracted driver throughout the state.[185]

(U) Although cell phone use is the most recognized distraction, all distractions inside a vehicle increase the likelihood of crashes or fatalities. Texas law prohibits drivers with a learners permit from using hand-held cell phone devices in the first six months of driving. Drivers under 18 are prohibited from using wireless communications while driving. School bus operators are restricted from texting and using hand-held devices while driving, and it is illegal for all drivers to text or use hand-held devices in school zones.[186] According to the Texas A&M Transportation Institute (TTI), almost half of all Texas drivers admit to regularly or sometimes talking or texting on a cell phone while driving.[187]

(U) The death of first responders, such as law enforcement officers and emergency medical personnel, also remains a concern. On September 1, 2003, Texas implemented the "Move Over" law. The law requires drivers who are approaching stopped emergency vehicles with activated lights to vacate the lane or slow to 20 miles per hour below the speed limit.[188] Since 2011, state legislators have added tow truck drivers and Texas Department of Transportation vehicles to the law.

(U) In 2015, 742 Texas crashes were reported that involved drivers violating the Move Over law, an increase from 644 in 2014. In 2015, Harris County had the highest number of such crashes with 123, followed by Dallas County with 119, Bexar County with 68, and Tarrant County with 50. From January 1 to April 30, 2016, 47 crashes occurred in Harris County, followed by Dallas County with 37, Bexar County with 33, and Tarrant County with 23.[189]

(U) According to Mason Dixon Polling & Research, 71 percent of Americans have never heard of Move-Over-type laws.[190] Additionally, a TTI study found that 40 percent of Texas drivers had not heard of the law.[191]

(U) Pedestrian-Related Fatal Crashes in Texas

(U) Many pedestrians share traveling space with motor vehicles crossing on roads or traveling on or alongside roads, too often with grave consequences, according to data. Pedestrian fatalities are rising. According to the National Traffic Highway Safety Administration, Texas ranked as the 10th most dangerous state for walking commuters.[192]

(U) In 2015, 554 pedestrian fatalities were reported in Texas, an increase from 495 in 2014. Most of them – 370 during 2015 – occurred when the victim failed to yield right of way to a vehicle. Of the 554 fatalities in 2015, 272 occurred between 6 p.m. and midnight. From January 1 to April 30, 2016, there were 185 pedestrian fatalities. Nearly half – 90 of them – occurred between 6 p.m. and midnight.

(U) Harris County reported the highest number of pedestrian fatalities in 2015, with 95, followed by Dallas County with 72, and Bexar County with 45. From January 1 to April 30, 2016, Harris County reported 45 pedestrian fatalities; Dallas County, 23; and Bexar County, 21.[193]

(U) The Texas Transportation Code requires that, in the event of a crash, every person involved in a crash immediately stop and determine whether the anyone require aid.[194] However, hit-and-run pedestrian fatalities increased, from 101 in 2014, to 113 in 2015. In 2015, Harris County had the highest number of hit and run pedestrian fatalities, with 30, followed by Travis County, with 13. From January 1 to April 30, 2016, Harris County again led the state with 12 hit and run pedestrian fatalities, followed by Dallas County, with five.[195]

3.1 Traffic Crash Risks in the Permian Basin Area

(U) The energy sector places significant demands on Texas' transportation system. Energy sector-related traffic can degrade roadways and other infrastructure,[196] and increases in oil and gas extraction have coincided with historically high numbers of crashes in rural regions. Crashes involving commercial vehicles may be caused by the commercial vehicle drivers or passenger vehicle drivers sharing the roadway, or other causes. The number of crashes and fatalities among both drivers and passengers seems to coincide with oil industry fortunes, which influences the number and variety of vehicles using roadways. Energy sector production continues at elevated rates in Texas, despite a recent period of relatively lower activity.

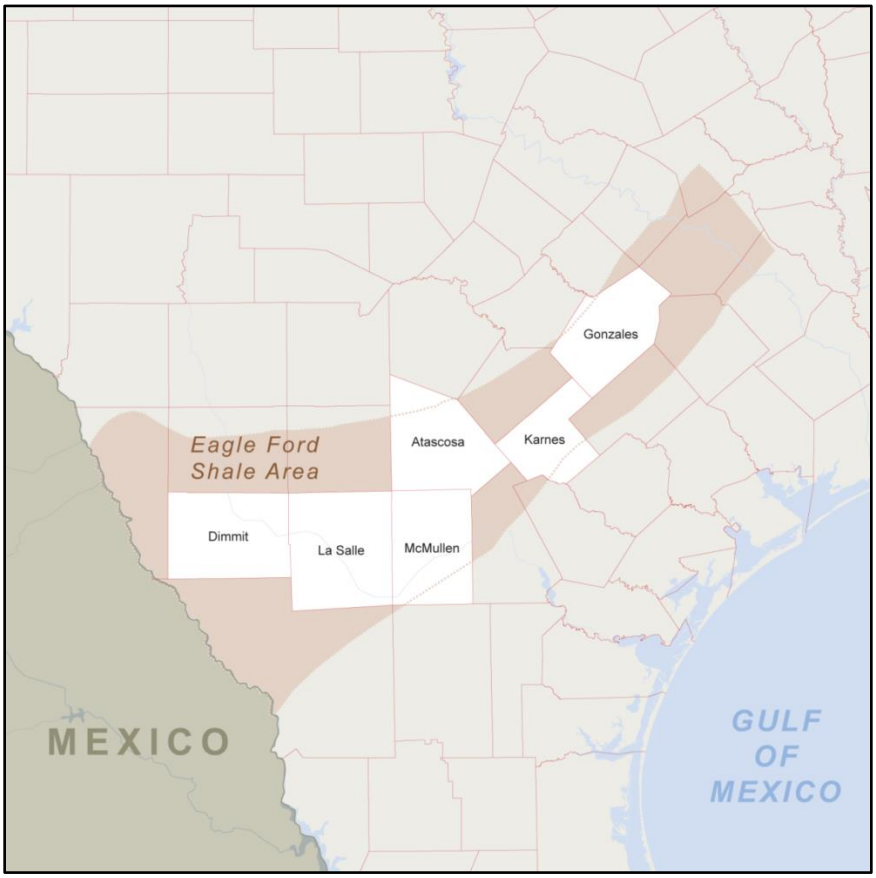
(U) The Permian Basin is an oil-and-gas-producing area of West Texas, and an adjoining part of southeastern New Mexico covering a region approximately 250 miles wide and 300 miles long. Increased drilling and extraction has produced a substantial economic boom that has increased and decreased with global commodities prices.[197] With the initial boom came significant increases in population, and vehicles of all weights traveling the roadways.[198]

(U) In 2013, the Permian Basin's drilling permitting and production increased substantially, with the number of permits rising from 8,872 to 10,966 in 2014, then decreasing by 60 percent in 2015 with oil price declines.[199] [200] [201]

(U) Coinciding with decreases in rig counts and permitting activity,[202] the number of motor vehicle crashes has declined 14 percent, from 12,276 crashes in 2014, to 10,548 in 2015. Fatal crashes declined from 291 in 2014, to 270 in 2015. Commercial vehicle-involved fatality crashes also decreased 15 percent, from 82 to 70. From January 1 to April 30, 2016, there were 60 fatal crashes resulting in 68 fatalities. Of the 60 fatal crashes, 16 involved a commercial vehicle.[203]

3.2 Traffic Crash Risks in the Eagle Ford Shale Area

(U) The Eagle Ford Shale (EFS), another of the state's major hydrocarbon-producing formations, extends across Texas from the Mexican border to East Texas. It is roughly 50 miles wide and 400 miles long.[204]



(U) As oil prices fell sharply in early 2015, the number of drilling permits declined 59 percent in the EFS area, from 5,613 permits to 2,315.[205] Coinciding with the statewide rig counts and permitting, fatality crashes in the region fell from 60 in 2015 to 41 in the early part of 2016. The number of CMV crashes fell from 619 to 462. From January 1 to April 30, 2016, there were eight fatal crashes resulting in eight fatalities. Of the eight fatal crashes, one involved a CMV.[206]

4. Natural Disasters

(U) Texas faces a diverse array of natural threats, including floods, tornadoes, tropical storms, hurricanes, droughts, wildfires, coastal erosion, land subsidence, dam and levee failure, and many types of severe weather. Texas has declared more major disaster declarations than any other state in the nation.[207] This assessment focuses on those natural hazards that are more likely to constitute homeland security threats and major public safety threats (i.e., create a large-scale response or sheltering demand) to Texas, either due to the frequency or impact of their occurrence. Due to the frequency of occurrence and higher impact, the ranking order of the top five hazards has changed since 2010. The table below lists and ranks the natural hazards facing the state, according to the 2013 State of Texas Hazard Mitigation Plan.

Natural Hazards	
1	Floods
2	Hurricane/Tropical Storms
3	Wildfire
4	Tornado
5	Drought
6	Coastal Erosion
7	Dam/Levee failure
8	Earthquakes
9	Expansive Soils
10	Extreme Heat
11	Hailstorm
12	Land Subsidence
13	Severe Winter Storms
14	Windstorms
15	Lightning

4.1 Floods

(U) Floods are defined as the accumulation of water within a water body and the overflow of excess water into adjacent floodplain lands.[208] On average, some 400 floods afflict Texas annually, and 91 percent of disaster damage in the state is related to flooding. Approximately 80 percent of the flooding in Texas occurs in the counties of Harris, Galveston, Brazoria, and Montgomery. While the accumulated damages from floods are severe, and occasionally require the deployment of swift-water rescue teams, most communities are able to handle the response to flooding with internal assets and local sheltering.

(U) Occurring mostly in the spring and fall, floods can last from a day to several months. In the event of a flood, areas are likely to expect a loss of transportation infrastructure and/or loss of citizens' homes. The warning time for a flood is generally between three and six hours but may be days on major river basins.

(U) As the most common disasters in Texas, floods can occur at any time of the year. In addition, riverine flooding is common, creating impacts far downstream from the initial flooding caused by rain. Examples of this include the massive flooding events in 2015, four of which were severe enough to require federal disaster declarations.

4.2 Tropical Storms and Hurricanes

(U) Tropical storms are areas of disturbed weather in the tropics with closed isobars and a distinct rotary circulation. Wind speeds range from 39 mph and 74 mph with heavy rain, localized flooding, high tides, localized coastal erosion, and minor wind damage. Hurricanes are classified into categories based on wind speed and the potential damage they can cause. To qualify as a hurricane, wind speeds must be greater than 75 mph. Thunderstorm rain resulting in urban flooding, battering wave action, intense sea level rising, localized coastal erosion, and significant winds are associated with hurricanes. Texas has had 20 federal major disaster declarations due to tropical storms and hurricanes since the 1950s. The 22 counties of the Gulf Coast, constituting 28 percent of the population of Texas, are the most vulnerable to tropical storms and hurricanes. The effect of Hurricane Gilbert, which made landfall in Mexico, illustrates that hurricanes need not actually cross the coastline to cause significant damage to our state. Damage from hurricanes is calculated from wind and storm surge flooding. Inland flood damage, caused by torrential

rains, is counted as riverine flood loss. Due to large-scale disruptions of the power grid, power outages can last for weeks. Storm surge flooding is typically the most deadly aspect of a hurricane.

(U) Based on the last 100 years of historical records, Texas should expect to see a land-falling hurricane an average of every two years, while any particular coastal community should expect to experience hurricane force winds about every 12 years, with a slightly higher incidence along the upper Texas coast. The hurricane season runs from June 1 through November 30, but in Texas, the peak occurs between July and September. Tropical storms and hurricanes last from a few hours to a few days. These storms occur with a minimum of a 12-hour warning. They cause power failures, destroy infrastructure, and interrupt telecommunications. The Saffir-Simpson Scale used to measure the intensity of storms is divided into categories 1-5, with category 1 being the least damaging.

(U) As mentioned, storms and hurricanes often lead to damaging floods. Hurricane Ike, for instance, hit the upper Texas Gulf Coast in September 2008, causing approximately $37 billion in damage. The hurricane left millions without power. Saltwater storm surges flooded most of the businesses and homes on Galveston Island, and many more along Galveston Bay.

4.3 Wildfires

(U) A wildfire is defined as a sweeping and destructive conflagration, especially in rural or wilderness regions. In Texas, with the semi-arid climate of the western, southern and panhandle counties of the state, wildfires are most common in the spring and summer months, but can occur at any time during the year. The eastern part of the state, also known as the Piney Woods, contains the most hazardous fuels in the state: pine plantations. Fires burning in this fuel type, when under drought conditions, can become extremely hard to contain, require multiple fire-fighting resources, and threatening all homes in their vicinity.

(U) Occurring mostly during dry seasons or droughts, and largely arising from forest, brush, and grass fires, wildfires can last from a few hours to a few weeks. Wildfires burn crops, kill livestock, destroy structures, down power lines, and cause road closures. The probability of wildland urban interface incidences has increased due to increased development in wildlands.

Livermore Ranch Wildfire, Jeff Davis County, 2012

(U) One condition required for a wildfire threat is dryness. The Keetch-Bryam Drought Index judges the expectation of a wildfire based on recent weather conditions and ranges from 0 to 800, with zero implying little to no expectation of a wildfire.

(U) Wildfires and flooding can go hand in hand. Flooding increases the growth of fuels to burn, and the effects of wildfires can create a greater risk of flooding. Normally, vegetation absorbs rainfall, reducing runoff. Wildfires leave the ground charred, barren, and unable to absorb water, creating conditions ripe for flash flooding and mudflow. Flood risk remains significantly higher until vegetation is restored – up to five years after a wildfire.[209]

(U) The response to large wildfires can be extensive, requiring shared human resources and assets from multiple local communities, and state and federal resources. In 2011, wildfires resulted in $500 million in wildfire and wildland urban interface damages. Law enforcement resources also are required for traffic

control during the active firefighting response phase, and to supervise re-entry of affected communities once the fire has been extinguished.

4.4 Tornadoes

(U) A tornado is defined as a rapidly rotating vortex or funnel of air extending from a cumulonimbus cloud. Texas averages 125 tornadoes annually, and the northern two-thirds of Texas are the most vulnerable to tornadoes. In late December 2015, a storm system over north Texas produced one of the most devastating and deadly winter tornado outbreaks in Texas history. Several thunderstorms produced 12 confirmed tornadoes across north Texas, with the most significant affecting the higher-population areas of eastern Dallas County into northwest Rockwall County, southeast Collin County, and Ellis County. This was the most tornadoes on record at once for north and central Texas since 1950.[210]

(U) Occurring mostly at night during the spring, tornadoes can last from a few minutes to two hours, although the resulting power outages can persist for days. Tornadoes occur with little forewarning and are likely to result in power failures. The Enhanced Fujita (EF) scale, which is used to measure the wind speed strength of a tornado, identifies tornados in six categories from 0 to 5, zero being the least damaging. Eighty percent of Texas tornadoes are ranked as either an F0 or an F1, with only one F5 per decade.

Damage in Rowlett, Texas, December 2015

(U) A tornado strike on a populated area will always require a significant response, causing the opening of community tornado safe rooms, responses to power outages, rescue operations, and debris removal and road clearing. Small communities normally require assistance from local partners or the state. Large communities generally only require outside assistance in the event of multiple touchdowns or in the event of the rare F3 or greater storms.

4.5 Drought

(U) Drought is defined as the consequence of a natural reduction in precipitation over an extended period of time, usually a season or more in length. Texas experienced a severe drought from 2010-2014 that ranked as the second worst and second longest statewide drought on record, based on the Palmer Drought Severity Index. The drought involved more than 80 percent of the state experiencing exceptional drought conditions at some point. The lack of rain and the high temperatures severely affected farmers and ranchers. Causing an estimated $5.2 billion in agricultural losses, the drought was one of the most costly on record. Losses included a $2.06 billion impact on livestock and a $3.18 billion impact on grains. Between March 2011 and the end of January 2012, nearly 100 percent of Texas was in some form of drought, based on data reported by the National Drought Mitigation Center. During the period of June through November 2011, 65 percent or more of Texas was in “exceptional” drought, the most severe level of drought.[211]

(U) Texas has experienced thousands of multi-county and regional disaster declarations as a result of drought. The area most vulnerable to drought is West Texas: the area encompassing Amarillo, Lubbock, Midland, Odessa, Fort Stockton, San Angelo, Laredo, and El Paso. From 1950 to 1957, Texas experienced the most severe drought in recorded history. By the time that drought ended, 244 of the 254

counties had been declared federal disaster areas. Based on the past occurrences of droughts and disaster declarations, estimated losses are mainly to crops and livestock, but can also affect local governments in higher maintenance costs on roads, parks, and water and waste-water systems, as well as additional costs to secure new water sources when those traditionally used run dry.

5. Public Health Threats

(U) Significant public health threats are possible throughout the state. Natural and industrial disasters can cause widespread damage, an array of acute injuries, chronic illnesses and mental health issues. Some disasters require evacuation of entire communities, placing significant stress on both the health of vulnerable populations and the healthcare systems of communities hosting evacuees. Emerging infectious diseases can spread through people, animal hosts, and even the food and water supply. These public health threats include mosquito-borne illnesses such as the West Nile and Zika viral diseases; respiratory illnesses such as influenza and Middle East Respiratory Syndrome (MERS); and bacterial diseases such as tuberculosis and salmonella.

5.1 Infectious Diseases

(U) Emerging and re-emerging infectious diseases are diseases that are either new, or previously recognized but re-emerging with new characteristics or in new areas. These diseases pose a potential threat to the health of Texans and have the potential to spread via people and products entering the state through international airports, ports of entry along the Gulf of Mexico, and the 1,200-mile international border with Mexico.[212] In addition, migratory birds and vectors such as mosquitoes and ticks may carry emerging diseases into and across the state. [213]

Arboviruses

(U) Texas is both an endemic and epidemic area for viruses transmitted by mosquitoes (arboviruses) including West Nile virus (WNV), St. Louis encephalitis virus (SLEV), Chikungunya virus (CHIKV), Dengue virus (DENV), and Zika virus (Zika). [214] [215] WNV and SLEV are maintained in nature through cycles involving mosquitoes and wild birds, while DENV, CHIKV, and Zika virus are maintained in a cycle involving humans and mosquitoes only. There are no specific antiviral treatments, and no human vaccines are commercially available in the US for any of these viral infections. Most human arbovirus cases occur from July through September when mosquitoes are most active.

Texas Arbovirus Trends, 2011-2015

Year	WNV Cases	SLEV Cases	CHIKV Cases	DENV Cases	Zika Cases
2011	27	0	NR	7	NR
2012	1,868	3	NR	16	NR
2013	183	1	NR	95	NR
2014	379	4	114	34	NR
2015	275	0	55	33	8

NR: No Reporting

West Nile virus (WNV)

(U) West Nile virus is a mosquito-borne illness that first emerged in Texas in 2002.[216] Since then, the virus has become endemic, with about 2,200 human cases reported during its first decade in the state, 2002–2011. [217] A severe WNV outbreak occurred in 2012. Although the Dallas-Fort Worth area was significantly impacted, WNV illnesses occurred across Texas, including 1,868 confirmed cases and 89 deaths during the 2012 transmission season. [218] There was a sharp decline in subsequent years. About one

in five WNV infected people will develop fever with other symptoms. Less than one percent of infected people develop a serious, sometimes fatal, neurologic illness.[219] There are no medications or vaccines to treat or prevent WNV infection.[220] West Nile virus is spread by the bite of an infected mosquito and can infect people, horses, many types of birds, and some other animals. The most common vectors for WNV are the *Culex pipens* and *Culex tarsalis* mosquitoes. There is no evidence that West Nile virus can be spread from person to person, or from animal to person. Transmission to humans is considered spillover from the natural cycle involving mosquitoes and wild birds. WNV risk may be reduced by removing standing water that could serve as a mosquito breeding ground, using insect repellent, wearing protective clothing, and staying indoors while mosquitoes are most active between dusk and dawn.

St. Louis encephalitis virus (SLEV)

(U) Saint Louis encephalitis virus (SLEV) is a mosquito-borne illness occurring in the eastern and central United States. Most persons infected with SLEV have no apparent symptoms or signs of illness. Initial symptoms can include fever, headache, nausea, vomiting, and malaise (tiredness). Severe neuroinvasive disease (often involving encephalitis, an inflammation of the brain) occurs more commonly in older adults. In rare cases, long-term disability or death can result. There is no specific treatment or vaccine for SLEV. [221] Like WNV, it is maintained in a mosquito-bird-mosquito cycle, with wild birds as primary hosts and *Culex* species mosquitoes transmitting it to humans. [222] SLEV risk may be reduced by removing standing water that could serve as a mosquito breeding ground, using insect repellent, wearing protective clothing, and staying indoors while mosquitoes are most active between dusk and dawn.

Chikungunya virus (CHIKV)

(U) Chikungunya virus is a mosquito-borne illness first identified in Texas in 2014 in a traveler. Cases have been identified in individuals with travel history to Africa, Asia, parts of Central and South America, and islands in the Indian Ocean, Western and South Pacific, and the Caribbean. With the exception of a single locally acquired case in 2015, all have been acquired outside of Texas. [223] The most common symptoms of CHIKV are fever and joint pain. Other symptoms may include headache, muscle pain, joint swelling, or rash. CHIKV is transmitted through mosquito bites only. When a mosquito feeds on an infected person the mosquito can become infected, then spreading the virus to the next person bitten. *Aedes aegypti* and *Aedes albopictus* mosquitoes spread CHIKV. These mosquitoes bite primarily during the daytime, both indoors and outdoors. They often live around buildings in urban areas. Wearing protective clothing can reduce the CHIKV risk to people, as can remaining inside air-conditioned buildings with window and door screens, and using insect repellent. [224]

Dengue virus (DENV)

(U) Dengue virus is a potentially severe mosquito-borne infection found in tropical and sub-tropical regions around the world. Texas cases are most often found in travelers, and are most frequently identified along the Texas–Mexico border. [225] DENV causes severe, flu-like illness that affects infants, young children, and adults, and can cause death. DENV is also known as "break bone fever," due to the additional symptoms of severe pain in the extremities. It also includes pain in the eyes and head, as well as respiratory inflammation. The primary vector of DENV is the *Aedes aegypti* mosquito, however the *Aedes albopictus* can also spread the disease. Both of these mosquitos are found in Texas. The virus is transmitted to humans through the bites of infected mosquitoes. After virus incubation for 4–10 days, an infected mosquito is capable of transmitting the virus for the rest of its lifespan. Infected humans are the main carriers, serving as a source of the virus for uninfected mosquitoes. Patients who are already infected with the DENV can transmit the infection (for 4–5 days; maximum 12) via *Aedes aegypti* mosquitoes after their first symptoms appear. These mosquitos bite primarily during the daytime, both indoors and outdoors, and often live around buildings in urban areas. DENV risk may be reduced by wearing protective clothing, staying inside air-conditioned buildings, controlling the mosquito population, and using insect repellent.

Zika virus (Zika)

(U) Zika virus disease (Zika) is caused by the Zika virus. It was first discovered in the Zika Forest of Uganda, and the first human cases were identified in 1952. Zika virus did not arrive in the Western Hemisphere until 2015 but quickly spread throughout South America, Central America, and across the Caribbean. By 2016, Texas was monitoring dozens of travelers arriving in the state with Zika virus infection and illness. The virus is spread to people primarily through the bite of an infected *Aedes* species mosquito, but can also be transmitted through sexual contact from infected men to their sex partners. The most common symptoms of Zika virus are fever, rash, joint pain, and conjunctivitis (red eyes). The illness is usually mild, with symptoms lasting for several days to a week after a bite from an infected mosquito. People ill with Zika virus typically do not require hospitalization, and rarely die. For this reason, many individuals may not realize that they have been infected. However, Zika virus infection during pregnancy may cause a serious birth defect called microcephaly, as well as other birth defects, such as defects of the eye, hearing deficits, and impaired growth. Zika virus may also cause Guillain-Barré syndrome (GBS), a rare condition of the nervous system in which a person's own immune system damages the nerve cells, causing muscle weakness, and sometimes, progressive paralysis. There are no medications to treat or vaccines to prevent Zika virus infection. Once a person has been infected, he or she is likely to be protected from future infections. Similar to CHIKV and DENV, Zika virus transmission is maintained in a cycle involving humans and mosquitoes only. *Aedes aegypti* and *Aedes albopictus* mosquitoes bite primarily during the daytime, both indoors and outdoors, and often live around buildings in urban areas. Zika virus risk may be reduced by protective clothing and by staying inside air-conditioned buildings. [226]

Viral Hemorrhagic Fevers

(U) Viral hemorrhagic fevers (VHFs) are a group of illnesses caused by several distinct families of viruses that result in similar effects. VHFs include, but are not limited to the Ebola, Marburg, Lassa, and Rift Valley Fever viruses. [227] In general, the term "viral hemorrhagic fever" describes a severe, multisystem syndrome that affects multiple organ systems in the body. Characteristically, the overall vascular system is damaged, and the body's ability to regulate itself is impaired. Symptoms are often accompanied by hemorrhage (bleeding); however, the bleeding in itself is rarely life-threatening. Severely ill patients may exhibit shock, nervous system malfunction, coma, delirium, and seizures. Some types of VHF are also associated with renal (kidney) failure. [228]

Ebola Virus Disease

(U) Ebola Virus Disease (EVD) is a rare and deadly disease caused by infection with one of the Ebola virus strains. Ebola can cause disease in humans and primates (monkeys, gorillas, and chimpanzees). The natural reservoir host of the Ebola virus remains unknown. [229] However, on the basis of evidence and the nature of similar viruses, researchers believe the virus is animal-borne, with bats being the most likely reservoir. Ebola viruses are found in several African countries. Ebola was first discovered in 1976 near the Ebola River in what is now the Democratic Republic of the Congo. Since then, outbreaks have appeared sporadically in Africa. Four of the five virus strains occur in animal hosts native to Africa. [230]

(U) When an infection does occur in humans, the virus can be spread in several ways to others. EVD is spread through direct contact (through broken skin or mucous membranes in the eyes, nose, or mouth) with body fluids of a person who is sick with Ebola, objects contaminated with the virus, or infected animals. EVD is not spread through air, water, or – in general – food. However, in Africa, EVD may be spread as a result of handling bush meat (wild animals hunted for food) and contact with infected bats. There is no evidence that mosquitoes or other insects can transmit the Ebola virus. Only certain mammals (for example, humans, bats, monkeys, and apes) have shown the ability to become infected with and spread EVD. There is no evidence that other mammals, such as dogs and cats, can develop the disease or spread the virus. [231]

(U) Healthcare providers caring for EVD patients and the family and friends in close contact with EVD patients are at the highest risk of becoming infected, as they may come in contact with the infected blood or body fluids of sick patients. During outbreaks of EVD, the disease can spread quickly within healthcare settings where hospital staff are providing close contact care or performing high risk procedures dealing with highly infectious patients. While the risk of transmission is fairly low, case fatality rates are typically high.

(U) 2014 Ebola Outbreak

(U) The 2014 Ebola outbreak in West Africa, first reported by the World Health Organization (WHO) on March 23, 2014, is the largest and most complex EVD outbreak since the virus was discovered in 1947. There were more cases and deaths in this outbreak than all others combined. By the end of the outbreak in March 2016, there were 28,616 confirmed EVD cases and 11,310 deaths. The three African countries most severely affected by the 2014 Ebola outbreak were Guinea, Liberia, and Sierra Leone, each of which have weak health systems and lack human and infrastructural resources. [232] On August 8, 2014, the WHO Director-General declared this outbreak a Public Health Emergency of International Concern. This declaration was lifted on March 29, 2016.[233]

(U) In September 2014, a Texas hospital patient tested positive for Ebola virus, marking the first EVD case diagnosed in the United States. The patient had recent history of travel from West Africa, and developed symptoms consistent with EVD days after arriving in Texas. The patient later died. Two healthcare workers who provided care to this patient subsequently became infected with EVD. [234] Both recovered. As the situation in West Africa continuously changed, Texas increased the monitoring of returning travelers in accordance with CDC guidelines and identified hospitals as Ebola Treatments Centers.

Respiratory Illnesses

(U) The virus most likely to cause a pandemic of respiratory illnesses is influenza A. However, other viruses, such as coronaviruses like the Middle East Respiratory Syndrome Coronavirus (MERS-CoV), also have pandemic potential.

Influenza

(U) Influenza (flu) is a contagious respiratory illness caused by influenza viruses. Flu can cause mild to severe illness. Serious outcomes of flu infection can result in hospitalization or death. Over a 30-year period, from 1977 to 2007, annual US flu-associated deaths ranged from a low of about 3,000 to a high of about 49,000 people. [235] Complications of flu can include bacterial pneumonia, ear infections, sinus infections, dehydration, and worsening of chronic medical conditions, such as congestive heart failure, asthma, and diabetes. Groups with the highest risk of developing severe complications from influenza include: [236]

- Young children (those younger than five, but especially those younger than two years old)
- Adults 65 or older
- Pregnant women
- Residents of long term care facilities and nursing homes
- Native Americans

(U) Most experts believe that flu viruses spread mainly by droplets created when people with flu cough, sneeze, or talk. These droplets can land on the mucus membranes of the mouths or noses of people who

are nearby. Less often, a person might also become infected with the flu virus by touching a surface or object that has the flu virus on it and then touching their own mouth, eyes, or nose.

(U) An annual seasonal flu vaccine is the best way to reduce the risks associated with seasonal flu outbreaks. When more people are vaccinated against the flu, less flu can spread through that community. Each year, the upcoming season's flu vaccine will protect against the influenza viruses research indicates will be most common during the season. For example, the 2016-2017 flu vaccine includes an influenza A (H1N1) virus, an influenza A (H3N2) virus, and one or two influenza B viruses, depending on the flu vaccine. [237]

(U) Antiviral drugs are important medical countermeasures for the influenza threat. Antiviral drugs are prescription medicines (pills, liquids, inhaled powders, or intravenous solutions) that fight the flu in those infected. They are available by prescriptions from health care providers. Antiviral drugs are different from antibiotics, which fight bacterial infections.

Middle East Respiratory Syndrome Coronavirus (MERS-CoV)

(U) MERS-CoV is a human coronavirus that leads to severe acute respiratory illness, including symptoms such as fever, cough, and shortness of breath. It is spread from an infected person's respiratory secretions through actions such as coughing. However, the precise ways the virus spreads are not completely understood. MERS-CoV was first reported in Saudi Arabia in 2012, and has since spread to several other countries, including the United States. Three to four of every 10 patients reported with MERS-CoV have died. [238]

(U) There is no vaccine available against MERS-CoV. There is also no specific antiviral treatment recommended for MERS-CoV infection, and patients are typically treated to help manage symptoms. For severe cases, current treatment includes care to support vital organ functions. The best way to reduce the risk of MERS-CoV infection is to follow respiratory disease precautions:

- Frequent handwashing with soap and water for 20 seconds, and help young children do the same – if soap and water are not available, an alcohol-based hand sanitizer can be used
- Using a tissue to covering the nose and mouth when coughing or sneezing, then disposing of it
- Avoiding touching the eyes, nose and mouth with unwashed hands
- Avoiding close personal contact, such as kissing, sharing drinking cups, or sharing eating utensils with sick people
- Frequent cleaning and disinfecting high-touch surfaces and objects, such as doorknobs

(U) In May 2014, the first confirmed cases of MERS-CoV in the United States were reported in two healthcare workers who had recently returned from Saudi Arabia. The two cases were not linked – one was in Indiana, and the other in Florida. Texas has not had any confirmed MERS-CoV cases.[239]

(U) Although MERS is a coronavirus causing serious illness, there are many more coronaviruses that produce very mild illness. In fact, most people become infected at some time in their life, resulting in mild to moderate upper-respiratory tract illnesses. Young children are more likely to become infected. Coronaviruses are also spread from an infected person to others through the air by coughing and sneezing, and close contact, such as touching or shaking hands, or caring for or living with an infected person. In the US, people usually become infected with common human coronaviruses in the fall and winter.

Bacterial Infections

Tuberculosis (TB) and Drug Resistant TB

(U) Tuberculosis is caused by the *Mycobacterium tuberculosis* bacteria. The bacteria usually attack the lungs, but TB bacteria can attack any part of the body, such as the kidneys, spine, and brain. Not everyone infected with TB bacteria becomes sick. As a result, two TB-related conditions exist: latent TB infection (LTBI) and TB disease. LTBI occurs when TB bacteria are in the body but suppressed by the immune system. Although an individual with LTBI does not display symptoms and is not infectious, TB disease can emerge when the individual's immune system is suppressed due to illness or age.[240] If not treated properly, TB disease can be fatal.

(U) It is estimated that one-third of the world's population is infected with TB. In 2014, 9.6 million people around the world became sick with TB disease, and 1.5 million died. In 2015, 1,334 cases of TB were reported in Texas, a rate of 4.9 per 100,000 people. This rate varies from state to state, ranging from 0.5 cases per 100,000 (West Virginia) to 9.1 cases per 100,000 (Alaska).[241] The overall rate for the US is 3.0 new cases per 100,000. TB can affect anyone, but is more likely to be diagnosed in people born in a foreign country where TB is prevalent, people living with diabetes or HIV/AIDS, homeless people, and health care workers. Alcohol abuse is associated with 17 percent of TB cases, and 10 percent of cases are diagnosed in detention facilities. A large-scale exposure to TB occurred between September 1, 2013 and August 16, 2014 at a hospital in El Paso, Texas.[242] The population exposed included hospital employees, newborns and infants, as well as members of the community who came into contact with people with active TB infection.

(U) TB is curable with proper treatment. However, some strains are resistant to the drugs used for treatment. In 2013, six people in Texas were diagnosed with multi-drug-resistant TB. One case of extensively drug resistant TB was also reported in Texas.[243]

Foodborne or Waterborne Illness

(U) Food- or water-related illnesses involve the unintentional or deliberate contamination of food or water that is consumed by humans. Food contamination can occur at any stage of food production, from farm to fork. An estimated 48 million people suffer from foodborne illnesses each year in the United States, accounting for 128,000 hospitalizations and approximately 3,000 deaths. About one in every six people will experience some sort of foodborne illness each year, and it is estimated that approximately five million Texas residents are at an increased risk due to conditions that compromise the immune system.[244]

(U) Cyclosporiasis is an intestinal illness caused by consuming food or water contaminated with the *Cyclospora* parasite. A recent surge in reports of illnesses due to the *Cyclospora* parasite has prompted the DSHS to begin an investigation into the infections in hopes of determining a common source.

(U) Some outbreaks in Texas are small and regionalized. Many of these small outbreaks are not recognized through routine public health surveillance, and go unreported. Other foodborne illnesses in Texas are traced to larger multi-state outbreaks with specific food items determined to be the source. In recent years, several food items have been determined to be the source of multi-state outbreaks, including *Salmonella* contamination of papayas in 2011, and serrano peppers in 2008. Salmonellosis cases have steadily increased in Texas from 2,819 cases in 2001 to 5,727 in 2015.[245] While the Texas and US food supplies are among the safest in the world, accidental or intentional contamination of food is always possible.

(U) There have been several high profile examples of deliberate food contamination in the US, including one in Texas. At a Dallas hospital in 1996, a disgruntled laboratory worker deliberately contaminated

food in a laboratory break room with *Shigella dysenteria* type 2, resulting in the illnesses of 12 coworkers.[246] Four victims were hospitalized, and five others were treated. Although there were no deaths, this incident demonstrates how food contamination can be used to deliberately harm others.

5.2 Other Recent Public Health Threats

Radiological Threats

(U) Almost every year, incidents are reported in Texas of the loss or theft of radioactive materials that are used in oil well drilling operations. Individuals who come into contact with these radiation sources, which can be unshielded, are susceptible to burns and sickness. Radioactive material was reported lost or stolen in 2011, and again in 2012, though in each case, it was subsequently found after extensive searches by the radiation licensee and the Texas Department of State Health Services.

Border Threats

(U) Texas shares a 1,254-mile international border with Mexico that includes 29 ports of entry. Many differences exist in environmental and product standards and regulations between the US and Mexico, which increases the risk of contaminated products being transported into Texas. The border can also serve as a gateway for individuals seeking to enter the US, either legally or illegally, carrying diseases ranging from influenza and TB to vaccine-preventable diseases (such as varicella or measles).

(U) In 2011, mercury-tainted face cream was transported into Texas, resulting in 45 poisonings, mostly among women residing near the border. The investigation indicated that the product was shipped from Mexico to businesses in Texas and other states. In addition to mercury, authorities also have discovered lead-contaminated products – such as toys and trinkets made in foreign countries – that can result in elevated blood lead levels in children.

6. Industrial Accidents

(U) The large industrial base in Texas generally operates safely, with minimal homeland security impact. However, due to the size and diversity of industries and their economic importance, any significant accidents could result in high consequences. Industrial accidents have the potential to threaten the state's security, especially when they result in casualties, the destruction of critical infrastructure, or the disruption of the state's economy.

(U) One significant incident that occurred recently was the collision between the M/V Summer Wind and the barge Kirby 27706 on March 22, 2014 in Galveston Bay. The barge was carrying over 900,000 gallons of fuel. Multiple coastal counties were impacted. Response was provided by local, state, private, and federal entities.[247]

(U) Railroad operations in Texas are another area of potential concern, given their importance to industries and the large volume of highly hazardous materials that are transported by railroad. Texas has an estimated 10,469 miles of freight railroad track. These rail lines pass through frontier, rural, suburban, and densely populated urban areas. In one city alone, over 500,000 people live within one mile of a railroad track. Texas is the largest origin point and termination destination for chemicals and petroleum products, and border and port areas pose special operating and capacity challenges for freight railroads.

7. Cyber Threats

(U) Technology has become a target, a vulnerability, and a tool used by criminals and terrorists. As a result, cyber threats have become increasingly significant areas of concern. A wide range of malicious cyber actors increasingly use cyberspace to overcome geography and traditional government defenses against malign cyber activity. At times, offensive operations have been driven by extremist ideology.

(U) Cyber threats, including cyber-terrorism, cyber-warfare, and cybercrime, range from benign, low-risk threats that are easily mitigated to high-risk threats requiring sophisticated countermeasures. Emerging and constantly changing technologies regularly provide new avenues of exploitation and create new areas of vulnerability that countermeasures must quickly match.

(U) We are concerned about the potentially severe consequences of an effective cyberattack against critical infrastructure facilities and systems, which could cause denial or disruption of essential services such as clean water distribution, energy distribution, public health systems, or law enforcement networks. In addition, cyberattacks could potentially facilitate extortion, intellectual property theft, and identity theft.

(U) Particularly vulnerable targets of hostile cyber actors are the aging legacy systems in use by state agencies and public sectors. Some of these systems lack adequate security controls, network monitoring and response, and identity and access management frameworks. Some agencies have instituted measures to address these vulnerabilities, but cyber threats can evolve at such a rapid pace that reducing vulnerability gaps will remain an ongoing challenge.

(U) Common kinds of malicious cyber activity include the use of botnets, distributed denial of service (DDoS), hacking, keystroke logging, malware, phishing, and webpage defacement.

7.1 Cyber Threat Actors

(U) The cyber threat is posed by many kinds of actors.

(U) Nations: Many developed and developing nations have built some form of offensive information-operations capability, and are constantly increasing resources to expand and maintain capabilities to further their perceived interests. Some nations appear organized and consistent in their targeting, both actively and retroactively operating to achieve a range of internal objectives. Some actively seek supply chain disruption. Others pursue espionage activities to support commercial or military interests.

(U) Cybercriminals: Cybercriminals are financially motivated, and seek to maintain access to systems to maximize their profits. They can range from individual actors to highly sophisticated multi-national operations. Cyber criminals use a variety of tactics and techniques as a part of multi-phased campaigns to obtain sensitive information that can be monetized. Some fraudulent schemes generate millions in criminal revenue annually. Criminal groups re-invest some of the proceeds of cybercrime to develop new technologies and systems to perpetuate the quality and complexity of cybercrime.

(U) Hacktivists: Hacktivists are politically or ideologically motivated cyber actors who can be independent or loosely organized. They can attack public and private sector networks to make a political point or effect change. They commonly conduct website defacements, redirects, denial-of-service attacks, information theft, virtual sabotage, and website parodies. They may or may not be tied to larger operational objectives.

(U) Terrorists and Ideological Organizations: Terrorists utilize cyberspace to conduct a full range of strategic and operational activities. Faced with increasing kinetic responses to overt activity, terrorists exploit the anonymity provided by cyberspace to conduct recruitment, encrypted terrorism planning, information operations, and financial management. Some organizations have ventured into cyberspace as a warfighting domain, employing assets in an offensive capability to support current operations.

(U) Insiders: Insider access can be a major enabler to cyber threat activity. Insiders have the potential to cause grave damage due to their access and knowledge of the system. They may be currently or previously employed by the agency or business that they are compromising. Often, the most significant vulnerability is an entity's failure to eliminate former employees' access to critical systems. Their intimate knowledge of programming, system, and access vulnerabilities allows disgruntled or malicious employees to cause lasting harm. The vulnerability is compounded by legacy or aging systems with little disaster recovery capability.

(U) Cyber Threats to the Electric Grid

(U) Critical infrastructure networks and connecting interoperable systems represent cyber targets of potentially high consequence for Texas, and we are concerned about the potential impact of a successful cyberattack on essential systems.

(U) On December 23, 2015 a regional electricity distribution company in the Ukraine reported widespread service outages to customers resulting from a third party's illegal entry into the company's computer systems.[248] While this event occurred in the Ukraine, it demonstrated that cyber threats to the electric grid are not hypothetical. The Ukraine attack was sophisticated and involved spear phishing and credential theft used to gain access to controlling computer systems, and data exfiltration to plan the attack.[249]

(U) The real-time flow of electricity on each grid is managed by control centers and energy control systems, which are uniquely designed and operated using Supervisory Control and Data Acquisition (SCADA) systems to control real-time physical processes that deliver continuous and reliable power throughout the grid.[250] In the Ukraine event, attackers gained access to collect system credentials and information to gain access the control system network. But, once inside, they demonstrated their ability to operate system components, confusing repair efforts and extending the outage time.[251]

(U) Electric power in Texas is provided over several separate grids. The Electric Reliability Council of Texas grid provides electric power to approximately 24 million customers representing about 90 percent of the state's electric load.[252] The Texas Panhandle and parts of East Texas are within the Eastern Interconnect, and far West Texas is within the Western Interconnect.[253] The consequences of a similar cyber-attack against any of these three grids would depend on many variables associated with the attack, as well as the level of resiliency built into the system and proactive protection measures. This Ukraine type of attack could potentially result in the disruption of electric power for localized areas or potentially wider areas of Texas. Any significant electric outage, left unrepaired over time, would potentially impact the state's economy, public health, and public safety.

(U) Cyberattacks may come from any number of sources and target many potential vulnerabilities. Perpetrators might include nation-state actors, non-state actors, insiders, criminal enterprises, or individual hackers.

Appendix 1: Texas Critical Infrastructure Sectors

(U) "Critical infrastructure" includes all public or private assets, systems, and functions vital to the security, governance, public health and safety, economy, or morale of the state or the nation.[254] Within Texas, major industries and facilities have been designated as critical to the national economy. For Texas and its economy, major disruptions in any one of these sectors can have serious cascading impacts on large numbers of people. Their protection, therefore, is a vital priority for the state.

Agriculture and Food

(U) The Agriculture and Food Sector consists of enterprises that grow crops, raise animals, harvest timber, fish and other animals from a farm, ranch, or their natural habitats. Food establishments transform livestock and agricultural products into products for intermediate or final consumption. The industry groups are distinguished by the raw materials (generally of animal or vegetable origin) processed into food and beverage products. The food and beverage products manufactured in these establishments are typically sold to wholesalers or retailers for distribution to consumers.

(U) Agriculture employs one of every seven Texans and contributes more than $100 billion to the state economy, including $6 billion in exports to foreign countries. According to the Texas Department of Agriculture, there are 247,500 farms in the state, totaling 130.4 million acres. Texas ranks first nationally in the amount of farmland and the production of cattle, sheep, goats, and cotton.

Chemical Sector

(U) The Chemical Sector is comprised of facilities that transform natural raw materials obtained from the earth, sea and air into products that are used every day, to include the transportation of these chemicals to intermediate or end users.

(U) In Texas, the Chemical Sector employs over 74,000 individuals and generates over 510,000 jobs indirectly through chemical manufacturing. These jobs total over $25.7 billion in earnings every year. Texas is home to the largest petrochemical cluster in the world. Houston alone accounts for over 42 percent of the nation's base petrochemical capacity. [255]

Commercial Facilities

(U) The Commercial Facilities Sector consists of commercial businesses and community facilities. Most are privately owned, but some are publicly owned and operated. This includes media and entertainment facilities, gambling facilities (casinos), lodging, outdoor event facilities, assembly locations, real estate facilities, and retail facilities.

(U) As of August 2012, the leisure and hospitality industry (which includes the arts, entertainment, recreation, hotels and other accommodations) employed 1.1 million individuals in the State of Texas, representing over 10 percent of jobs.

Communications Sector

(U) The Texas Communications Sector consists of establishments that operate, maintain, and provide access to facilities that transmit voice, data, text, sound and video. These facilities may be based on

multiple technologies, including wired communications, wireless communications, satellite communication, the Internet, information services, next-generation networks and others.

Dams Sector

(U) The Dams Sector encompasses dam projects, flood damage reduction systems, hurricane and storm surge protection systems, mine tailings, industrial waste impoundments, and other water retention and water control facilities.

(U) There are 7,310 dams in Texas, 50 percent of which are less than 25 feet in height and 94 percent of which are 50 feet or less in height.[256] Most of these dams are earthen structures built before 1980. The U.S. Army Corps of Engineers reports that 1,856 (25 percent of the dams in Texas) are considered to have either "significant" or "high" hazard potential.[257] Although the state relied heavily on power from dams in the 1930's, other forms of power generation such as coal and natural gas, have transcended hydroelectric power as energy sources. Hydroelectric power accounts for less than one percent of the electricity generated in Texas.[258]

(U) A more important role of state dams is to control flooding and prevent property damage. Dam breaks can cause extensive damage downstream, and a major concern regarding their safety is their age. The National Inventory of Dams notes that most of the dams in Texas were built many decades ago: 271 dams were built before 1900, another 852 predate 1950, 1,089 were built in the 1950s, and 2,740 dams were built in the 1960s.[259]

(U) A number of Texas dams, experienced increased risk during 2015 and 2016 from heavy rainfall and flooding across the state. In the last part of May 2015, approximately a dozen homes were threatened when the dam on Pandera Lake near Midlothian when water passed over the top of the earthen dam.[260] On May 25, 2016, a century old dam in Bastrop State Park was overtopped and failed.[261] During the May 2015 flooding event, the Lewisville Dam north of Dallas, experienced a 160-foot-long slide causing concern of the dam's overall safety.[262] Heavy rainfall over the Houston area in April 2016 led to widespread flooding, stressing the Addicks and Barker dams and increasing concern about their ability to protect Houston from additional flooding.[263] This in turn, threatened the heavily populated residential areas downstream in the Houston area.

Defense Industrial Base

(U) The Defense Industrial Sector consists of the Department of Defense, government, and private sector industrial complex that perform research and development, and also design, produce, and maintain military weapons systems and parts.

(U) Fort Hood is the largest single-site employer in Texas, with more than 52,000 assigned personnel and 9,600 civilian employees. One of every 10 active duty soldiers in the US Army is assigned to Fort Hood, and the 335-square mile base is ranked first among the army's 97 installations in terms of future capability. The base directly contributes more than $3 billion to the Texas economy each year; in 2005, the Texas Comptroller estimated that the overall benefit of Fort Hood to the Texas economy exceeded $6 billion.

(U) From 2000 to 2007, 11,658 Texas companies contracted with the Department of Defense for a total of $197.1 billion, with $39.5 billion in 2007 alone. In 2007, Texas was second only to Virginia in the ranking of states by total defense-contract values. Defense spending has increased dramatically in Texas over the last decade, and has provided Texas with high-wage jobs with averages of $50,000 a year, as well as additional work for thousands of smaller companies such as subcontractors and suppliers.

Emergency Services

(U) The Emergency Services Sector consists of assets involved in emergency response designed to save lives, protect property and the environment, assist in the management of disasters (both natural and manmade) and aid in recovery. According to the DHS, this sector includes law enforcement, fire, emergency medical services, emergency management, and public works entities.[264]

(U) Texas has a robust network of emergency services that encompasses 1,875 fire departments and 1,913 law enforcement agencies.[265] Statewide, emergency management entities include 24 disaster districts and a state level Emergency Management Council encompassing 33 state agencies and voluntary organizations.[266]

(U) Texas is divided into 22 trauma service areas (TSAs), with a regional advisory council (RAC) in each region that develops and implements a regional trauma system plan. Two RACs have been approved as regional trauma systems, and there are 290 designated trauma facilities – including 17 Level I (Comprehensive) Trauma Centers.[267] Overall, Texas has 649 hospitals with 84,000 licensed beds.[268]

Energy

(U) The Texas Energy Sector consists of assets that relate to producing or supplying energy. It includes assets and facilities that produce or supply electricity, petroleum, natural gas, ethanol, biodiesel, hydrogen, coal, and renewable energies.

(U) Texas is the leading crude oil producer in the United States; the state's 29 petroleum refineries process over 5.4 million barrels of crude oil per day, which accounts for more than one-fourth of all domestic refining capability. Likewise, more than one-fourth of all US natural gas production occurs in Texas, making it the nation's leading natural gas producer. Texas has 263,729 intrastate and

interstate regulated miles of oil and gas industry pipelines, according to the Texas Railroad Commission.[269]

(U) Texas leads the nation in renewable energy potential, with large amounts of wind and solar generation capacity. Texas now has the most wind generation capacity in the country, accounting for one fifth of the national total. With its large population, extensive industrial sector, and hot climate, Texas consumes more electricity than any other state.

Financial Services

(U) The Financial Services Sector consists of establishments primarily engaged in financial transactions (transactions involving the creation, liquidation, or change in ownership of financial assets) and/or in facilitating financial transactions. In Texas, it is comprised of two primary sub-sectors: banking and insurance. It includes establishments for banking and credit, securities and commodities, insurance, and other financial establishments.

(U) As of March 2016, the Texas Department of Banking regulated 1,094 entities, including 250 state-chartered banks and 194 national banks. The state-chartered and national banks safeguard a combined $302 billion in deposits and $363 billion in assets. In 2015, Texas licensed 1,815 insurance companies, regulated by the Texas Department of Insurance. During 2014, Texas consumers paid $139.2 billion in premiums, while insurers paid Texas policyholders $97.9 billion in claims.[270] [271]

Government Facilities

(U) The Government Facilities sector consists of buildings and structures associated with and owned, leased, or otherwise acquired by federal, state, local, tribal and territorial government agencies. These buildings and structures provide personnel, service, research, storage and preservation, sensor and monitoring, space system, military and education oriented facilities.

(U) The Texas Facilities Commission manages and provides planning for over 28 million square feet of property and facilities in more than 283 cities across Texas.[272] TFC supports the needs of over 62,600 state employees.[273] Texas has 8,656 public and chartered schools serving 5.2 million children.[274] Including branches and bookmobiles, the state's 875 libraries serve a population of 22.6 million people. The Texas Department of Criminal Justice maintains facilities for the incarceration of approximately 150,000 offenders.[275]

Information Technology

(U) The Information Technology (IT) sector consists of physical assets and virtual systems and networks that enable key capabilities and services in both the public and private sectors. Functions are sets of processes that produce, provide, and maintain products and services. These functions encompass the full set of processes involved in creating IT products and services, including research and development, manufacturing, distribution, upgrades, and maintenance. They also support the sector's ability to produce and provide high-assurance products, services, and practices that are resilient to threats and can be rapidly recovered. Critical IT Sector facilities, operations, and services provide for the design, development, distribution, and support of IT products (hardware and software). The IT Sector also provides operational support services that are essential or critical to maintain or reconstitute IT Sector critical functions.

(U) The Texas Department of Information Resources (DIR) is responsible for the statewide leadership and oversight for the management of government information and communications technology.

(U) The official *eGovernment* Internet portal for Texas, "Texas.gov," provides more than 1,000 online services such as driver license and vehicle registration renewals, capital access, and licensing for concealed handguns. From its inception in 2000 through 2015, Texas.gov has had over 240 million site visits, processed nearly 245 million financial transactions, collected over $33 billion on behalf of Texas public entities, and contributed over $223 million to the Texas State Treasury.[276]

Manufacturing

(U) The Manufacturing Sector consists of establishments engaged in the mechanical, physical or chemical transformation of materials, substances, or components into new products. These establishments include factories, mills, and plants. Manufacturing includes: food, beverage, tobacco, textiles, wood products, paper, petroleum/coal, chemical, plastics/rubber, non-metal minerals, metals, computer/electronics, machinery, transportation, furniture, mining and oil/gas extraction. The assembling of component parts of manufacture products is considered manufacturing, except in cases where the activity is appropriately categorized in construction.

(U) Establishments in this sector are often described as plants, factories or mills, and characteristically use power-driven machines and material-handling equipment. However, establishments that transform materials or substances into new products by hand or in the worker's home and those engaged in selling to the general public products made on the same premises from which they are sold, such as bakeries, candy stores, and custom tailors, may also be included in this sector. Manufacturing establishments often perform one or more activities that are categorized outside this sector.

(U) Texas accounts for over $251 billion worth of exported manufactured goods during 2015, ranking as the number one exporter in the nation.[277] Texas ranks second in the manufacture of computers and electronic equipment[278], and second in chemicals (but leading in the production of benzene, ethylene, fertilizers, propylene, and sulfuric acid). Seven percent of the nation's food-processing workers are located in Texas, making it the second largest contributing state, with beverages as majority products. Beer, soft drinks, baked goods, preserved fruits and vegetables, and meat are all important processed products for Texas. Texas leads the states in the total value of its mined products, producing large quantities of oil and natural gas. Additionally, Texas ranks seventh amongst the states in non-fuel mineral production value for items such as cement, crushed stone, lime, salt, sand and gravel.[279]

Nuclear Reactors, Materials, and Waste

(U) In Texas, the Nuclear Reactors, Materials and Waste sector principally consists of (1) commercial nuclear reactor for generating electric power and non-power nuclear reactors used for research, testing, and training; (2) nuclear materials in medical, industrial, and academic settings and facilities that fabricate nuclear fuel; and (3) the transportation, storage, and disposal of nuclear materials and radioactive waste.

(U) The Nuclear Regulatory Commission's Region IV Office in Arlington is responsible for carrying out the agency's duties in Texas. Texas is an agreement state in which the state has assumed authority to license and regulate byproduct materials, source materials, and certain quantities of special nuclear materials.[280] The State has two nuclear plants with two reactors each (Comanche Peak operated by Luminant in Glen Rose and the South Texas Project in Palacios). In addition to these two reactors, there are two research and test reactors located on the campus of Texas A&M University and the University of Texas at Austin. The annual nuclear energy production for Texas is 5.1GW.[281]

(U) Uranium deposits in Texas are found in relatively narrow bands that parallel the coastline. There are seven uranium in-situ-leach plants in Texas with a combined production capacity of 7.3 million pounds each year. At the end of 2015 two of these plants were operating, three in restoration status, one was in standby status, and one was permitted and licensed.[282] In 2009, a new low-level nuclear waste storage facility was licensed for operation by Waste Control Specialists to accept low-level nuclear waste from other states.

Public Health and Healthcare

(U) The Public Health and Healthcare sector consists of assets associated with the provision of health-related services to individuals (generally referred to as "healthcare"). It also includes assets associated with the provision of health-related services to populations, such as the general community, workplaces, academic institutions, and the military (generally referred to as "public health"), and the provision of health-related supporting services. It includes both public and private facilities.

(U) Health and human services in Texas are provided by several agencies: the Health and Human Services Commission, the Department of Family and Protective Services, the Department of Aging and Disability Services, and the Department of State Health Services. These agencies spend more than $30 billion a year, with the administration of over 200 programs and the employment of approximately 56,500 state workers[283] in over 1,300 locations around the state.

Transportation Systems

(U) Texas' Transportation Sector consists of a multitude of networks of transportation systems. A 2015 state data report by the Bureau of Transportation Statistics indicated that Texans drive an average of 645 million miles every day. As of 2015, the economic impact of transportation on employment was an average of 390,221 jobs. Transportation infrastructure statistics include: 313,228 miles of public roads, 3,415 miles of interstates, 52,898 bridges, 10,469 miles of freight railroad track, 830 miles of inland waterways, and 382 public-use airports. Seven of the top 50 water ports (by total tonnage) in the United States are in Texas.[284]

(U) Since 1990, Texas' population increased by 55 percent and road use grew by 110 percent, but the state's road capacity grew by just 7 percent. The Texas Department of Transportation estimates that the state's population will increase to 45 million by 2040. Continued population increases are expected to present challenges for the transportation system in Texas, forcing the state to increase capacity, repair deteriorating infrastructure facilities, decrease or at least control traffic congestion, and address safety issues – while also meeting state and federal air pollution standards.[285]

Water and Wastewater

(U) The Water and Wastewater sector is concerned with various aspects of water, such as the supply, transmission, storage of raw water, physical and chemical treatment facilities, treated water storage, distribution centers, monitor and distribution control centers, wastewater facilities, and regulatory organization for the system.

(U) Texas has three state agencies with jurisdiction over water issues:

- The Texas Water Development Board is responsible for planning and funding projects that enhance water availability;
- The Texas Commission on Environmental Quality is responsible for protecting the state's water quality and allocating the use of surface water;
- The Texas Parks and Wildlife Department ensures that the state's wildlife, including the vital fish, shrimp, and oyster industries, have sustainable supplies of fresh water.

(U) Groundwater, which represents half of water use in Texas, is not managed by any state agency.

(U) Texas has 191,000 miles of rivers and streams that provide about 40 percent of the total water used in the state (15.5 million acre-feet in 2004); and 23 surface water basins, 15 of which are major river basins and 8 of which are coastal river basins. There are 196 lakes in Texas, but only one of them is not man-made: Caddo Lake in East Texas. Water used for human consumption in municipalities is piped to water treatment plants that filter and chemically treat the water to bring it to drinking water standards, and then pumped through water delivery pipes to the end users. Treatment and distribution is an energy-intensive process – up to 80 percent of treatment costs are due to electricity consumption.

(U) Treated drinking water is distributed by various entities including municipal water services, in most urban areas: municipal utility districts (MUDs), authorized by the Texas Commission on Environmental Quality (TCEQ) at the request of property owners and by private water supply companies. In Texas, TECQ enforces the federal laws that set quality standards for such water systems, including the Clean Water Act and the Safe Drinking Water Act.

Appendix 2: Contributing Agencies

Countless agencies contributed to the production of this assessment and work together on an ongoing and regular basis. This collaboration underscores the commitment among agencies to share information in order to enhance public safety. Some of these agencies are listed below, as are agencies that participate in Operation Border Star and contributors to the TxGang database.

Agencies participating in Operation Border Star are listed below:

El Paso JOIC Sector

USBP
CBP – OFO
ICE
West TX HIDTA
EPIC
TMF
DPS
TPWD
ATF
FBI
TSA
USMS
US Diplomatic Security Service
Veteran Administration PD
US Army, Ft. Bliss CID
US Army, Ft. Bliss 902 MI
US Army, Ft. Bliss Emergency Management
El Paso CO SO
Dona Ana CO SO (NM)
Grant CO SO (NM)
Hidalgo CO SO (NM)
Luna CO SO (NM)
Otero CO SO (NM)
Anthony PD
El Paso PD
Horizon City PD
Socorro City PD
Ysleta Del Sur Tribal PD
El Paso ISD PD
University of Texas El Paso PD
El Paso Community College PD
El Paso Office of Emergency Management
El Paso County Juvenile Probation
El Paso Fire Department
Texas Tech University PD
Texas Comptroller of Public Accounts
Texas Attorney General, El Paso
BNSF Railroad PD
Union Pacific Railroad PD
Texas Alcoholic Beverage Commission
El Paso County Constables
National Drug Intelligence Center

Marfa JOIC Sector

USBP
CBP - OFO
ICE /HSI
NPS
TPWD
DPS
Brewster CO SO
Culberson CO SO
Hudspeth CO SO
Jeff Davis CO SO
Pecos CO SO
Presidio CO SO
Reeves CO SO
Terrell CO SO
Alpine PD
Fort Stockton PD
Pecos PD
Presidio PD

Del Rio JOIC Sector

CBP-OFO
DEA
DPS
FBI
HSI-ICE
IBWC
NPS
South TX HIDTA
Texas Military Forces
Zavala Co Constable
TPWD
USBP
USCG
USMS
Crystal City PD
Del Rio PD
Dimmit CO SO
Maverick CO SO
Uvalde CO SO
Val Verde CO SO
Zavala CO SO
38th Judicial Dist.
Dimmit CO Constable PCT 2
Dimmit CO Constable PCT 3
Edwards CO SO
Kinney CO SO
Real CO SO
Uvalde PD

Laredo JOIC Sector

USBP
CBP – OFO
DEA
FBI
ICE
USMS
Federal Protective Services
Army Intel
Union Pacific Railroad PD
TAMIU PD
TPWD
TMF
DPS
Duval CO SO
Frio CO SO
Jim Hogg CO SO
La Salle CO SO
Webb CO SO
Constable Pct. 3
Constable Pct. 4
Zapata CO SO
Freer PD
Dilley PD
Laredo PD
Pearsall PD
San Diego PD
LISD PD
UISD PD

Rio Grande Valley JOIC Sector

CBP – USBP
CBP – OFO
ATF
ICE / HSI
IBWC
NICB
USCG
US Fish & Wildlife
Brownsville HIDTA
DPS
TPWD
TDCJ
Brooks CO SO
Cameron CO SO
Hidalgo CO SO
Kenedy CO SO
Starr CO SO
Starr CO DA's Office
Hidalgo CO Pct 1
Hidalgo CO Pct 2
Hidalgo CO Pct 3
Hidalgo CO Pct 4
Willacy CO SO
Willacy CO DA's Office
Alamo PD
Brownsville PD
Donna PD
Edcouch PD
Elsa PD
Edinburg PD
Falfurrias PD
Harlingen PD
Hidalgo PD
Laguna Vista PD
La Feria PD
La Grulla PD
La Joya PD
La Villa PD
Lyford PD
Los Fresnos PD
Mercedes PD
Mission PD
Palmhurst PD
Palmview PD
Penitas PD
Pharr PD
Rancho Viejo PD
Raymondville PD
Rio Grande City PD
Roma PD
San Benito PD
San Juan PD
Sullivan City PD
UTPA PD
UTB PD
Weslaco PD

Coastal Bend JOIC Sector

USBP
ICE / HSI
FBI
ATF
USCG
US Fish and Wildlife
US Parks Service-PINS
US Postal Inspector
Union Pacific Railroad PD
TPWD
TXDOT
Houston HIDTA
San Antonio HIDTA
TMF
DPS
TX Attorney General's Office
Aransas CO SO
Bee CO SO
Calhoun CO SO
Dewitt CO SO
Goliad CO SO
Gonzales CO SO
Guadalupe CO SO
Jackson CO SO
Jim Wells CO SO
Karnes CO SO
Kleberg CO SO
Lavaca CO SO
Matagorda CO SO
Live Oak CO SO
Matagorda CO SO
McMullen CO SO
Nueces CO SO
Nueces Constable Pct. 3
Refugio CO SO
San Patricio CO SO
Victoria CO SO
Wharton CO SO
Alice PD
Bay City PD
Beeville PD
Corpus Christi PD
Corpus Christi PA
Cuero PD
Driscoll PD
El Campo PD
George West PD
Hallettsville PD
Kingsville PD
Kingsville Task Force
Orange Grove PD
Premont PD
Point Comfort PD
Port Lavaca PD

Refugio PD	Seguin PD	Three Rivers PD
Robstown PD	Sinton PD	Victoria PD
Rockport PD	Taft PD	Yoakum PD

DPS recognizes the following agencies for their contribution to the Texas Gang Investigative Database (TxGang), as of 2015:

Abilene Police Department
Addison Police Department
Alice Police Department
Alief Independent School District Police Department
Allen Police Department
Alvin Independent School District Police Department
Aransas Pass Police Department
Arlington Police Department
Austin Pardon and Parole Board
Austin Police Department
Bastrop County Sheriff's Office
Baytown Police Department
Beaumont Police Department
Beeville Police Department
Bexar County Community Supervision and Corrections
Bexar County Sheriff's Office
Big Spring Police Department
Brazoria County Sheriff's Office
Brazos County Juvenile Probation Department
Brenham Police Department
Bryan Police Department
Carrollton Police Department
Center Police Department
Cleveland Independent School District Police Department
College Station Police Department
Comal County Sheriff's Office
Conroe Independent School District Police Department
Conroe Police Department
Cooke County Sheriff's Office
Corinth Police Department
Corpus Christi Police Department
Cypress Fairbanks Independent School District Police Department
Dallas Area Rapid Transit Police Department
Dallas District Attorney's Office
Dallas Police Department
Denton County Sheriff's Office
Denton Police Department
Dumas Police Department
Edgewood Independent School District Police Department
Edinburg Police Department
El Paso Police Department
Ellis County Sheriff's Office
Erath County Sheriff's Office
Euless Police Department

Farmers Branch Police Department
Federal Bureau of Investigation
Forney Police Department
Fort Bend County Sheriff's Office
Fort Worth District Attorney's Office
Fort Worth Police Department
Frisco Police Department
Gainesville Police Department
Galveston County Sheriff's Office
Galveston Police Department
Garland Police Department
Georgetown Police Department
Gladewater Police Department
Goose Creek Consolidated Independent School District Police Department
Gregg County Sheriff's Office
Guadalupe County Sheriff's Office
Haltom City Police Department
Hamilton Police Department
Hansford County Sheriff's Office
Harker Heights Police Department
Harlingen Police Department
Harris County Constables Office - Precinct 1
Harris County Sheriff's Office
Hays County Gang Task Force
Hays County Sheriff's Office
Hidalgo County Sheriff's Office
Hondo Police Department
Houston County Sheriff's Office
Houston District Attorney's Office
Houston Fire Department Arson Bureau
Houston Independent School District Police Department
Houston Metropolitan Transit Authority Police Department
Houston Police Department
Humble Independent School District Police Department
Irving Police Department
Katy Independent School District Police Department
Katy Police Department
Kaufman Police Department
Kenedy Police Department
Kerr County Sheriff's Office
Killeen Police Department
Kleberg County Sheriff's Office
Klein Independent School District Police Department
La Marque Police Department
La Porte Police Department
La Salle County Sheriff's Office
Lacy Lakeview Police Department
Lake Dallas Police Department
Lancaster Police Department
Laredo Police Department
Lewisville Police Department

Liberty County Sheriff's Office
Liberty County Community Supervision and Corrections Department
Liberty District Attorney's Office
Livingston Police Department
Longview Police Department
Lorena Police Department
Lubbock County Constable's Office – Precinct 2
Lubbock County Sheriff's Office
Lubbock Police Department
Lufkin Police Department
Mansfield Police Department
Marble Falls Police Department
McKinney Police Department
McLennan Community College Police Department
McLennan County Community Supervision and Corrections Department
McLennan County Juvenile Probation Office
McLennan County Sheriff's Office
Mesquite Police Department
Midland Police Department
Missouri City Police Department
Montgomery County Constable's Office – Precinct 3
Montgomery County Constable's Office – Precinct 5
Montgomery County Juvenile Probation Department
Montgomery County Sheriff's Office
Nacogdoches County Sheriff's Office
Nacogdoches Police Department
New Braunfels District Attorney's Office
New Braunfels Police Department
New Caney Independent School District Police Department
Nueces County Sheriff's Office
Oak Ridge North Police Department
Odessa Police Department
Onalaska Police Department
Parker County Sheriff's Office
Pasadena Police Department
Pearland Police Department
Pflugerville Independent School District Police Department
Pflugerville Police Department
Pharr Police Department
Plano Police Department
Port Aransas Police Department
Port Arthur Police Department
Primera Police Department
Quinlan Police Department
Randall County Sheriff's Office
Refugio County Sheriff's Office
Richardson Police Department
Rockwall County District Attorney's Office
Rockwall County Sheriff's Office
Rosenberg Police Department
Round Rock Police Department

Sachse Police Department
Saginaw Police Department
San Angelo Police Department
San Antonio District Attorney's Office
San Antonio Police Department
San Juan Police Department
San Marcos Police Department
Santa Fe Police Department
Seagoville Police Department
Seguin Police Department
Shelby County Sheriff's Office
Sherman Police Department
Smith County Sheriff's Office
Socorro Independent School District Police Department
Spring Branch Independent School District Police Department
Spring Independent School District Police Department
Sugar Land Police Department
Temple Police Department
Texas City Police Department
Tom Green County Sheriff's Office
Tomball Police Department
Travis County Sheriff's Office
Tyler Police Department
US Bureau of Alcohol, Tobacco, Firearms, and Explosives
US Customs and Border Protection
US Immigration and Customs Enforcement
US Marshals Service
University Of Texas - Houston Police Department
Uvalde Police Department
Val Verde County Sheriff's Office
Victoria County Juvenile Probation Department
Victoria County Sheriff's Office
Victoria Police Department
Vidor Police Department
Waco District Attorney's Office
Waco Police Department
Webster Police Department
Wichita Falls Police Department
Williamson County Attorney's Office
Williamson County Sheriff's Office
Williamson County Juvenile Services
Wood County Sheriff's Office
Yoakum Police Department

References

[1] (U) FBI Assistant Director Michael B. Steinbach Statement Before the House Homeland Security Committee, 3 June 2015, https://www.fbi.gov/news/testimony/terrorism-gone-viral-the-attack-in-garland-texas-and-beyond
[2] (U) US v Kareem, Case 2:15-cr-00707-SRB, indictment, document 1 and superseding indictments document 57 and 158
[3] (U) "Report: Shooters at Garland Texas Muhammad cartoon event linked to ISIS," Newsweek, 4 May 2015, http://www.newsweek.com/report-shooters-garland-texas-muhammad-cartoon-event-linked-isis-328267
[4] Both San Bernardino attackers pledged allegiance to the Islamic State, officials say," The Washington Post, 8 December 2015, https://www.washingtonpost.com/news/post-nation/wp/2015/12/08/both-san-bernardino-attackers-pledged-allegiance-to-the-islamic-state-officials-say/
[5] (U) "Always Agitated. Always Mad: Omar Mateen, According to Those Who Knew Him," The New York Times, 18 June 2016, http://www.nytimes.com/2016/06/19/us/omar-mateen-gunman-orlando-shooting.html?rref=collection%2Fnewseventcollection%2F2016-orlando-shooting&action=click&contentCollection=us&region=rank&module=package&version=highlights&contentPlacement=1&pgtype=collection
[6] (U) Statement of US House Homeland Security Committee ChairmanTexas Rep. Michael McCaul, 14 July 2016
[7] (U) "Paris attacks show cracks in France's counterterrorism effort," The Wall Street Journal, 23 November 2015, http://www.wsj.com/articles/paris-attacks-show-cracks-in-frances-counterterrorism-effort-1448244796
[8] (U) "EU's Border Agency Admits Terrorists Are Exploiting Refugee Crisis and Lax Controls," The Daily Mail, 5 April, 2016, http://www.dailymail.co.uk/news/article-3525279/Mass-migration-allowing-terrorists-pour-Europe-EU-s-border-agency-admits-s-revealed-false-documents-not-facing-thorough-checks.html
[9] (U) "How the Paris bomber sneaked into Europe: Terrorist posing as a refugee was arrested and fingerprinted in Greece – then given travel papers and sent on his way to carry out suicide bombing in France," The Daily Mail, 16 November 2015, http://www.dailymail.co.uk/news/article-3320272/Paris-bomber-sneaked-Europe-posing-refugee-Greece-arrival-given-travel-papers-officials-admit-damning-expose-EU-s-open-borders-policy.html
[10] (U) "Master bombmaker who posed as migrant and attacked Paris last year is now chief suspect in Belgian atrocity as police swoop on home district," The Daily Mail, 22 March 2016, http://www.dailymail.co.uk/news/article-3504920/Master-bombmaker-posed-migrant-attacked-Paris-year-chief-suspect-Belgian-atrocity-police-swoop-home-district.html
[11] (U)"Five Syrian asylum seekers surrender at Texas border crossing," The Los Angeles Times, 21 November 2015, http://www.latimes.com/nation/la-na-syrians-border-20151121-story.html
[12] (U) "Tracing the path of four terrorists sent to Europe by the Islamic State," The Washington Post, 22 April 2016, https://www.washingtonpost.com/world/national-security/how-europes-migrant-crisis-became-an-opportunity-for-isis/2016/04/21/ec8a7231-062d-4185-bb27-cc7295d35415_story.html
[13] (U) "Swiss confirm arrest of three Iraqis for suspected support of Islamic State," The Wall Street Journal, 31 October 2014, http://www.wsj.com/articles/swiss-confirm-arrest-of-three-iraqis-for-suspected-support-of-islamic-state-1414758169
[14] (U) "Germany investigating 40 ISIL suspects who entered country posing as refugees," The Telegraph, 11 May 2016, http://www.telegraph.co.uk/news/2016/05/11/germany-investigating-40-isil-suspects-who-entered-country-posin/
[15] (U) Chemnitz bombing plot: German police searching for Syrian refugee on suspicion of planning terror attack," The Independent, 8 October 2016, http://www.independent.co.uk/news/world/europe/chemnitz-bombing-plot-germany-police-syrian-refugee-jaber-al-bakr-planning-terror-attack-a7351711.html; "German terror manhunt ends as police arrest Syrian refugee," The Wall Street Journal, 10 October 2016, http://www.marketwatch.com/story/german-terror-manhunt-ends-as-police-arrest-syrian-refugee-2016-10-10
[16] (U) "Swiss confirm arrest of three Iraqis for suspected support of Islamic State," The Wall Street Journal, 31 October 2014, http://www.wsj.com/articles/swiss-confirm-arrest-of-three-iraqis-for-suspected-support-of-islamic-state-1414758169
[17] (U) "ISIS bomb plotter's tour of Britain: Afghan 'refugee' suspected of planning terror attacks used fake IDs to visit high-profile UK sites and posed for pictures as he scouted for targets," The Daily Mail, 11 May 2016

[18] (U) "Syrian ISIS supporter shot dead outside Paris police station had been arrested for sexually assaulting women in Cologne and may have taken part in New Year's Eve attacks," The Daily Mail, 11 January 2016, http://www.dailymail.co.uk/news/article-3393516/Syrian-ISIS-supporter-shot-dead-outside-Paris-police-station-arrested-sexually-assaulting-women-Cologne-taken-New-Year-s-Eve-attacks.html#ixzz43zVdoLiR
[19] (U) "Germany investigating 40 ISIL suspects who entered country posing as refugees," The Telegraph, 11 May 2016, http://www.telegraph.co.uk/news/2016/05/11/germany-investigating-40-isil-suspects-who-entered-country-posin/
[20] (U) A Syrian Christian, seeking asylum, wonders why he's in custody in Texas," The Los Angeles Times, 20 December 2015, http://www.latimes.com/nation/la-na-texas-syrian-refugees-20151219-story.html
[21] (U) Department of Justice, District of Maryland Press Release, "Ocean City Man Sentenced for Immigration Fraud," 26 February 2014, https://www.justice.gov/usao-md/pr/ocean-city-man-sentenced-immigration-fraud
[22] (U) US Government Accountability Office report 16-50, "Additional Actions Needed to Assess and Address Fraud Risks," 2 December 2015, http://www.gao.gov/products/GAO-16-50
[23] (U) "Report: US-bound Syrians arrested in Honduras with fake passports," USA Today, 19 November 2015, http://www.usatoday.com/story/news/world/2015/11/18/report-us-bound-syrians-arrested-honduras-fake-passports/76016812/
[24] (U) A Syrian Christian, seeking asylum, wonders why he's in custody in Texas," The Los Angeles Times, 20 December 2015, http://www.latimes.com/nation/la-na-texas-syrian-refugees-20151219-story.html
[25] (U) "Iraqi Christians held for months by ICE after crossing Mexican border in asylum bid," Fox News, 6 August 2015, http://www.foxnews.com/us/2015/08/06/iraqi-christians-held-for-months-by-ice-after-crossing-mexican-border-in-asylum.html
[26] (U) United States v. Rakhi Gauchan, Complaint, Document 3, 3:14-cr-0068-DCG Western District of Texas
[27] (U) United States v. Dhakane, Government Sentencing Memorandum, Document 57, 5:10-cr-00194-XR, Western District of Texas
[28] (U) United States v. Fessahazion, Plea Agreement, Document 23, 4:09-cr-00498, Southern District of Texas
[29] (U) US Department of Justice, "Iranian Convicted of Running Profitable Alien Smuggling Operation in South America, October 3, 2002.
[30] (U) USA v Omar Faraj Saeed Al Hardan, Case 4:16-cr-00003, Document 1, Southern District of Texas, Houston Division, 7 January 2016.
[31] (U) FBI chief warns 'terrorist diaspora' will come to the West," Bloomberg News, 27 July 2016, http://www.bloomberg.com/news/articles/2016-07-27/fbi-chief-warns-terrorist-diaspora-will-be-coming-to-the-west
[32] (U) Worldwide Threat Assessment of the US Intelligence Community. Senate Armed Services Committee. James R Clapper, Director of National Intelligence. 26 February 2015.
[33] (U) "Countering Violent Islamist Extremism: The Urgent Threat of Foreign Fighters and Homegrown Terror". Hearing before the House Committee on Homeland Security. Nicholas J. Rasmussen, Director, National Counterterrorism Center. February 11, 2015.
[34] (U) "Current Terrorist Threat to the United States". Hearing before Senate Select Committee on Intelligence. Nicholas J. Rasmussen, Director, National Counterterrorism Center. February 12, 2015.
[35] (U) "Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations." Michael Steinbach, Counterterrorism Division, Federal Bureau of Investigation. 26 February 2015.
[36] (U) FBI chief warns 'terrorist diaspora' will come to the West," Bloomberg News, 27 July 2016, http://www.bloomberg.com/news/articles/2016-07-27/fbi-chief-warns-terrorist-diaspora-will-be-coming-to-the-west
[37] (U) IntelCenter, "Islamic State (IS) activity unprecedented in history of terrorism," 10 May 2016, http://intelcenter.com/reports/islamic-state-records/index.html#gs.j0mSdg8
[38] (U) "ISIS attacks around the world," The New York Times, 17 June 2015, http://www.nytimes.com/interactive/2015/06/17/world/middleeast/map-isis-attacks-around-the-world.html?_r=0
[39] (U) "ISIS attacks around the world," The New York Times, updated 16 July 2016, http://www.nytimes.com/interactive/2016/03/25/world/map-isis-attacks-around-the-world.html
[40] (U) "Philadelphia police officer wounded in ambush on his patrol car," The New York Times, 9 January 2016, http://www.nytimes.com/2016/01/09/us/philadelphia-police-officer-wounded-in-ambush-on-his-patrol-car.html
[41] (U) "Terrorism Threat Snapshot," Majority Report of the US Congress Committee on Homeland Security, 7 July 2016

[42] (U) Statement of National Counterterrorism Center Director Nicholas J. Rasmussen, Hearing before the House Homeland Security Committee "Worldwide Threats to the Homeland: ISIS and the New Wave of Terror" 14 July 2016
[43] (U) FBI chief warns 'terrorist diaspora' will come to the West," Bloomberg News, 27 July 2016, http://www.bloomberg.com/news/articles/2016-07-27/fbi-chief-warns-terrorist-diaspora-will-be-coming-to-the-west
[44] (U) "Countering Violent Islamist Extremism: The Urgent Threat of Foreign Fighters and Homegrown Terror". Hearing before the House Committee on Homeland Security. Nicholas J. Rasmussen, Director, National Counterterrorism Center. February 11, 2015.
[45] (U) "Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations." Michael Steinbach, Counterterrorism Division, Federal Bureau of Investigation. 26 February 2015.
[46] (U) "Always Agitated. Always Mad: Omar Mateen, According to Those Who Knew Him," The New York Times, 18 June 2016, http://www.nytimes.com/2016/06/19/us/omar-mateen-gunman-orlando-shooting.html?rref=collection%2Fnewseventcollection%2F2016-orlando-shooting&action=click&contentCollection=us&region=rank&module=package&version=highlights&contentPlacement=1&pgtype=collection
[47] "Omar Mateen was 'inspired' by ISIS, President Obama says," WFTV9ABC, 1 July 2016, http://www.wftv.com/news/pulse-shooting/omar-mateen-was-inspired-by-isis-said-president-obama/342896446
[48] (U) "White House says Texas shooting was attempted terror attack," CNN, 5 May 2015, http://www.cnn.com/2015/05/05/politics/white-house-texas-terror/
[49] (U) "Everything we know about the San Bernardino Attack," The Los Angeles Times, 14 December 2015, http://www.latimes.com/local/california/la-me-san-bernardino-shooting-terror-investigation-htmlstory.html
[50] (U) "Ohio man arrested in alleged plot to attack Capitol," The Washington Post, 14 January 2016, https://www.washingtonpost.com/world/national-security/ohio-man-arrested-in-alleged-plot-to-attack-capitol/2015/01/14/044e9ca8-9c36-11e4-96cc-e858eba91ced_story.html
[51] (U) "Ottawa Gunman's Radicalism Deepened as Life Crumbled," The New York times, 24 October 2014, http://www.nytimes.com/2014/10/25/world/americas/ottawa-canada-gunmans-radicalism-deepened-as-life-crumbled.html?_r=0
[52] (U) "Hit-and-Run That Killed Canadian Soldier Is Called Terrorist Attack," The New York Times, 21 October 2014, http://www.nytimes.com/2014/10/22/world/americas/canadian-soldier-run-down-in-what-officials-call-act-of-terror-dies.html
[53] (U) "Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations." Michael Steinbach, Counterterrorism Division, Federal Bureau of Investigation. 26 February 2015.
[54] (U) "NYC officials reassure residents after ISIS video shows Times Square, praises Paris attackers," Fox News, 19 November 2015, http://www.foxnews.com/us/2015/11/19/new-isis-video-threatens-to-attack-times-square-in-new-york-city/
[55] (U) "Police: Seattle man's hatred of U.S. foreign policy motivated killings," CNN, 16 September 2014,http://www.cnn.com/2014/09/16/justice/ali-brown-charges-killing-spree/
[56] (U) "NJ student's accused killer also charged with 3 murders in Wash.," CBS News New York, 21 August 2014 http://www.cbsnews.com/news/new-jersey-students-accused-killer-also-charged-with-three-murders-in-washington/
[57] (U) *DABIQ magazine*; Issue 6; 1436 Rabi al-Awwal.
[58] (U) "NYPD, D.C. Police Probe Ax Attacks on Officers," CBS New York, 31 October 2014, http://newyork.cbslocal.com/2014/10/31/nypd-d-c-police-probe-ax-attacks-on-officers/
[59] (U) Press Release DC Metropolitan Police Department "Suspect Sought in Assault on a Police Officer: 1200 block of Quincy St. NE. 31 October 2014, http://mpdc.dc.gov/release/suspect-sought-assault-police-officer-1200-block-quincy-st-ne
[60] (U) "UCC posts names, addresses of 1,500 purported Texas residents: 'Shoot them down'," SITE Intelligence Group, Dark Web & Cyber Security, 2 May 2016, https://ent.siteintelgroup.com/Dark-Web-and-Cyber-Security/ucc-posts-names-addresses-of-1-500-purported-texas-residents-shoot-them-down.html
[61] (U) "From Amateur to Ruthless Jihadist in France," The New York Times, 17 January 2015, http://www.nytimes.com/2015/01/18/world/europe/paris-terrorism-brothers-said-cherif-kouachi-charlie-hebdo.html

[62] (U) "How Europe's migrant crisis became an opportunity for ISIS," The Washington Post, 22 April 2016, https://www.washingtonpost.com/world/national-security/how-europes-migrant-crisis-became-an-opportunity-for-isis/2016/04/21/ec8a7231-062d-4185-bb27-cc7295d35415_story.html
[63] Ibid.
[64] (U) "Paris Attacks Plot Was Hatched in Plain Sight," The Wall Street Journal, 27 November 2015, http://www.wsj.com/articles/paris-attacks-plot-was-hatched-in-plain-sight-1448587309
[65] (U) "France: Suspected Mastermind of 13 November Paris Attacks Said He Entered France Two Months Earlier, Paris Valeurs Actuelles, translated by the Open Source Center, 27 November 15, 2015
[66] (U) "The mystery surrounding the Paris bomber with the fake Syrian passport," The Washington Post, 17 November 2015, https://www.washingtonpost.com/world/europe/the-mystery-surrounding-the-paris-bomber-with-a-fake-syrian-passport/2015/11/17/88adf3f4-8d53-11e5-934c-a369c80822c2_story.html?hpid=hp_rhp-top-table-high_migrants-845pm:homepage/story
[67] (U) "Paris Attacks Show Cracks in France's Counterterrorism Effort," The Wall Street Journal, 23 November 2015, http://www.wsj.com/articles/paris-attacks-show-cracks-in-frances-counterterrorism-effort-1448244796
[68] (U) US v. Michael Todd Wolfe, aka "Faruq," Case No. A14-M-288, Criminal Complaint, US District Court for the Western District of Texas.
[69] (U) US v. Rahatul Ashkim Khan, Case No. A-14-M-285, Criminal Complaint, US District Court for the Western District of Texas.
[70] (U) USA v Omar Faraj Saeed Al Hardan, Case 4:16-cr-00003, Document 1, Southern District of Texas, Houston Division, 7 January 2016.
[71] (U) USA v Omar Faraj Saeed Al Hardan, Case 4:16-cr-00003, Document 1, Southern District of Texas, Houston Division, 7 January 2016.
[72] (U) "Houston man pleads guilty to supporting ISIL," KHOU News, 17 October 2016, http://www.khou.com/news/crime/houston-man-pleads-guilty-to-supporting-isil/337085505
[73] (U) US v. Bilal Abood, Criminal Complaint, Case 3-15-MJ-316, Northern District of Texas, 13 May 2015.
[74] Ibid.
[75] (U) US v. Asher Abid Khan, Criminal Complaint, Case H15-712, Southern District of Texas, 25 May 2015.
[76] Ibid.
[77] (U) US Identifies Citizens Joining Rebels in Syria, Including ISIS," The New York Times, 28 August 2014, http://www.nytimes.com/201/08/29/world/middleeast/us-identifies-citizens-joining-rebels-in-syria.html
[78] (U) "Countering Violent Islamist Extremism: The Urgent Threat of Foreign Fighters and Homegrown Terror". Hearing before the House Committee on Homeland Security. Nicholas J. Rasmussen, Director, National Counterterrorism Center. February 11, 2015.
[79] (U) Homeland Security Committee, Terror Threat Snapshot: April 2016. Majority Staff of the Homeland Security Committee, April 2016.
[80] (U) Homeland Security Committee, Terror Threat Snapshot: April 2016. Majority Staff of the Homeland Security Committee, April 2016.
[81] (U) US House of Representatives Homeland Security Committee, "Final Report of the Task Force on Combating Terrorist and Foreign Fighter Travel." September, 2015, https://homeland.house.gov/wp-content/uploads/2015/09/TaskForceFinalReport.pdf
[82] (U) USA v Hamza Naj Ahmed, Mohamed Abdihamid Farah, Adnan Abdihamid Farah, Abdurahman Yasin Daud, Zacharia Yusuf Abdurahman, Hanad Mustofe Musse, and Guled Ali Omar Case Number 0:15-cr-00049-MJD-FLN (7 suspects);USA v Bilal Abood, Case Number 3-15-MJ-316 BK (1 suspect); USA v Sinh Vinh Ngo Nguyen Case Number 2:13-cr-00736-JFW (1 suspect); USA v Liban Haji Mohamed, a.k.a, "Shirwa," "Shirwac," "Qatiluhum," "Qatil," and "Abu Ayrow" Case Number 1:14mj64 (1 suspect).
[83] (U) Saadiq Long, et al, versus Loretta Lynch, in her official capacity of Attorney General of the United States, US District Court Eastern District of Virginia Alexandria Division, case 1:15-cv-01642-LO-MSN, Document 9, Defendants' Memorandum of Law in Opposition to Plaintiff's Emergency Motion for a Temporary Restraining Order, filed 12/17/15
[84] (U) United States versus Jason Michael Ludke and Yosvany Pedilla-Conde, criminal complaint case No. 16-M-162, US Attorney's Office, Eastern District of Wisconsin, https://www.justice.gov/opa/file/903066/download
[85] (U) "Sheriff: ISIS Recruits Arrested North of San Angelo," San Angelo Live news report, 4 October 2016, http://sanangelolive.com/news/crime/2016-10-14/sheriff-isis-recruits-arrested-north-san-angelo

[86] (U) United States versus Jason Michael Ludke and Yosvany Pedilla-Conde, criminal complaint case No. 16-M-162, US Attorney's Office, Eastern District of Wisconsin, https://www.justice.gov/opa/file/903066/download
[87] (U) "FBI: 2 men wanted to join ISIS," The Milwaukee Journal Sentinel, 14 October 2016, http://www.jsonline.com/story/news/crime/2016/10/14/2-milwaukee-men-charged-terrorism-related-crimes/92073802/
[88] (U) USA. V. Hamza Naj Ahmed et al Superseding Indictment dated 05/18/2015, Case 15-mj-312 BRT, District of Minnesota
[89] Ibid.
[90] (U) USA v. Bilal Abood, Criminal Complaint, Case 3-15-MJ-316, Northern District of Texas, 13 May 2015
[91] Ibid.
[92] (U) USA v. Sinh Vinh Ngo Nguyen aka "Hasan Abu Omar Ghannoum", Case CR 13-0736 JFW, Central District of California
[93] (U) USA v. Sinh Vinh Ngo Nguyen aka "Hasan Abu Omar Ghannoum" Plea Agreement dated 12/20/2013, Case CR 13-0736 JFW, Central District of California
[94] (U) Goldman, Adam and Zapotosky, "Virginia cabbie on FBI's Most Wanted Terrorists list detained in Somalia", Washington Post, March 2, 2015
[95] (U) FBI Most Wanted Terrorists "Liban Haji Mohamed" DOI January 29, 2015 https://www.fbi.gov/wanted/wanted_terrorists/liban-haji-mohamed
[96] (U) Goldman, Adam and Zapotosky, "Virginia cabbie on FBI's Most Wanted Terrorists list detained in Somalia", Washington Post, March 2, 2015
[97] (U) "Houston-area man arrested in undercover FBI terrorism sting," Reuters News Service, 28 March 2014, http://www.reuters.com/article/us-usa-crime-texas-sting-idUSBREA2S00S20140329
[98] (U) "Police: Austin shooter was a 'homegrown American extremist'" The Washington Post, December 1, 2014 http://www.washingtonpost.com/news/post-nation/wp/2014/12/01/police-austin-shooter-belonged-to-an-ultra-conservative-christian-hate-group/
[99] (U)) "Police: Austin shooter was a 'homegrown American extremist'" The Washington Post, December 1, 2014 http://www.washingtonpost.com/news/post-nation/wp/2014/12/01/police-austin-shooter-belonged-to-an-ultra-conservative-christian-hate-group/
[100] Ibid.
[101] "Animal testing company Mary Kay cosmetics sabotaged," North American Animal Liberation Press Office, 5 October 2014.
[102] (U); CNN; "Who is Gavin Long?"; 4 AUG 2016; http://www.cnn.com/2016/07/18/us/who-is-gavin-long/; accessed on 8 AUG 2016; (U) New source.
[103] (U); The Wall Street Journal; "Black Separatist Group Denies Connection to Baton Rouge Gunman?"; 18 JUL 2016; http://www.wsj.com/articles/black-separatist-group-denies-connection-to-baton-rouge-gunman-1468878762; accessed on 8 AUG 2016; (U) New source.
[104] (U) Number of law enforcement officers fatally shot this year up significantly after ambush attacks, report says," The Washington Post, 27 July 2016, https://www.washingtonpost.com/news/post-nation/wp/2016/07/27/number-of-law-enforcement-officers-fatally-shot-this-year-up-significantly-after-ambush-attacks-report-says/?utm_term=.4cebc550bec0
[105] (U) Ambushes of Police: Environment, Incident Dynamics, And the Aftermath of Surprise Attacks," US Department of Justice Community Oriented Policing Services, Fachner, George; Thorkildsen, Zoe, http://ric-zai-inc.com/Publications/cops-p340-pub.pdf
[106] (U) "Suspect in Police Shootings Carries Lengthy Arrest Resume," U.S. News, 22 December 2014, http://www.usnews.com/news/newsgram/articles/2014/12/22/ismaaiyl-brinsley-arrested-19-times-before-shooting-pair-of-nypd-officers-in-brooklyn
[107] (U) "Two admit plot to blow up police station, St. Louis County prosecutor, Ferguson police chief," The St. Louis Post-Dispatch, 2 June 2015, http://www.stltoday.com/news/local/crime-and-courts/two-admit-plot-to-blow-up-police-station-st-louis/article_47bc72ff-ad16-5ce7-b7be-432180fa555e.html
[108] (U) "Sheriff links 'Black Lives Matter' movement to slain deputy," CBS News, 31 August, 2015, http://www.cbsnews.com/news/darren-goforth-killing-sheriff-cites-black-lives-matter-movement/

[109] (U) "Investigators: Suspected Tennessee Gunman Motivated By Incidents Involving Police, Blacks," WJLA Washington D.C., 08 July 2016, http://wjla.com/news/nation-world/investigators-suspected-tennessee-highway-gunman-motivated-by-recent-police-shootings
[110] (U) "Man fires 17 shots into officer's patrol car and home, screams he hates police," Fox 59 News, 12 July 2016, http://fox59.com/2016/07/12/police-man-fires-more-than-a-dozen-shots-into-home-car-of-impd-officer/
[111] (U) "Credible" plot to kill Baton Rouge police officers foiled", CBS News, 12 July 2016, http://www.cbsnews.com/news/alton-sterling-alleged-plot-to-kill-baton-rouge-police-foiled/
[112] (U) "Investigators: Suspected Tennessee Gunman Motivated By Incidents Involving Police, Blacks," WJLA Washington D.C., 08 July 2016, http://wjla.com/news/nation-world/investigators-suspected-tennessee-highway-gunman-motivated-by-recent-police-shootings
[113] (U) "Before Dallas, another shooting targeting police," CNN, 8 July 2016, http://www.cnn.com/2016/07/08/politics/dallas-police-shooting-bristol-tennessee/
[114] (U) "Investigators: Suspected Tennessee Gunman Motivated By Incidents Involving Police, Blacks," WJLA Washington D.C., 08 July 2016, http://wjla.com/news/nation-world/investigators-suspected-tennessee-highway-gunman-motivated-by-recent-police-shootings
[115] Ibid.
[116] (U) "Authorities: Tennessee Highway Gunman motivated by police shootings," Tribune News Services, 8 July 2016, http://www.chicagotribune.com/news/nationworld/ct-tennessee-highway-shooting-20160708-story.html
[117] (U)"HCSO: Suspect Arrested, Charged In Shooting Death Of Sheriff's Deputy," Click 2 Houston, 30 August 2015, http://www.click2houston.com/news/hcso-suspect-arrested-charged-in-shooting-death-of-sheriffs-deputy_20151123153749801
[118] (U) "Deputy Killed In Houston Ambush Shot 15 Times; Suspect Held Without Bond," Dallas News, 31 August 2015, http://www.dallasnews.com/news/state/headlines/20150831-deputy-killed-in-houston-ambush-shot-15-times-suspect-held-without-bond.ece
[119] (U) "Sheriff links 'Black Lives Matter' movement to slain deputy," CBS News, 31 August, 2015, http://www.cbsnews.com/news/darren-goforth-killing-sheriff-cites-black-lives-matter-movement/
[120] (U) "Indictment in deputy's death cites retaliation as motive," The Houston Chronicle, 23 November 2015, http://www.houstonchronicle.com/news/houston-texas/houston/article/Indictment-in-deputy-s-death-cites-retaliation-as-6653004.php
[121] (U) "Motive Revealed in Deadly Shooting of Deputy Darren Goforth," 23 November 2015, KPRC Houston News, http://www.click2houston.com/news/motive-revealed-in-deadly-shooting-of-deputy-darren-goforth
[122] (U) "Deputy Killed In Houston Ambush Shot 15 Times; Suspect Held Without Bond," Dallas News, 31 August 2015, http://www.dallasnews.com/news/state/headlines/20150831-deputy-killed-in-houston-ambush-shot-15-times-suspect-held-without-bond.ece
[123] (U) "Suspect in Police Shootings Carries Lengthy Arrest Resume," U.S. News, 22 December 2014, http://www.usnews.com/news/newsgram/articles/2014/12/22/ismaaiyl-brinsley-arrested-19-times-before-shooting-pair-of-nypd-officers-in-brooklyn
[124] Ibid.
[125] (U) "Two admit plot to blow up police station, St. Louis County prosecutor, Ferguson police chief," The St. Louis Post-Dispatch, 2 June 2015, http://www.stltoday.com/news/local/crime-and-courts/two-admit-plot-to-blow-up-police-station-st-louis/article_47bc72ff-ad16-5ce7-b7be-432180fa555e.html
[126] (U) United States District Court, Eastern District of Missouri, Eastern Division, document titled "Superseding Indictment: United States of America v. Olajuwon Davis and Brandon Orlando Baldwin," 01 April 2015
[127] (U) "Two Local Men Sentenced On Federal Explosives And Weapons Charges," Federal Bureau of Investigation, 03 September, 2015, https://www.fbi.gov/stlouis/press-releases/2015/two-local-men-sentenced-on-federal-explosives-and-weapons-charges
[128] (U) "Two with Black Panthers connections charged in St. Louis bomb plot," The St. Louis Post-Dispatch, 21 November 2014, http://www.stltoday.com/news/local/crime-and-courts/two-with-black-panther-connections-charged-in-st-louis-in/article_bc0d3aea-f21d-5e29-947b-5c777ec2d70d.html
[129] (U) "Two admit plot to blow up police station, St. Louis County prosecutor, Ferguson police chief," The St. Louis Post-Dispatch, 2 June 2015, http://www.stltoday.com/news/local/crime-and-courts/two-admit-plot-to-blow-up-police-station-st-louis/article_47bc72ff-ad16-5ce7-b7be-432180fa555e.html
[130] (U) Texas Department of Public Safety. "Crime in Texas: 2015". September 2016.

[131] (U) Ibid.
[132] (U) Texas Human Trafficking Prevention Task Force Report to the Texas Legislature. December 2012.
[133] (U) FBI Law Enforcement Bulletin. *Human Sex Trafficking*. March 2011. http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/march_2011/human_sex_trafficking
[134] (U) US Immigration and Customs Enforcement. Houston man charged with transporting a child for commercial sex. July 25, 2012. http://www.ice.gov/news/releases/1207/120725houston.htm
[135] https://www.justice.gov/usao-sdtx/pr/four-ordered-prison-sex-trafficking-minors
[136] (U) KSLA Staff Email. "3 arrested in human trafficking bust, including runaway teen". *KSLA News*. December 18, 2014.
[137] (U) United States Attorney's Office: Southern District of Texas. Houston Man Charged with Sex Trafficking of a Minor. August 28, 2013.
[138] https://www.justice.gov/usao-wdtx/pr/new-mexico-man-sentenced-federal-prison-sex-trafficking-children
[139] http://texaspolicenews.com/default.aspx/act/newsletter.aspx/category/News+1-2/Startrow/71/MenuGroup/Home/NewsletterID/61175.htm
[140] (U) Assessing the Threat of Human Trafficking in Texas. Texas Department of Public Safety. March 2014.
[141] Texas Penal Code, Title 5, Chapter 20A, http://www.statutes.legis.state.tx.us/Docs/PE/htm/PE.20A.htm
[142] (U) Texas Attorney General's Office. "The Texas Human Trafficking Prevention Task Force Report 2012". December 2012.
[143] (U) United States Attorney's Office: Eastern District of Texas. Houston Couple Sentenced in Chinese Restaurant Employment Conspiracy. February 6, 2015.
[144] (U) United States Attorney's Office: Eastern District of Texas. Arrests Made In Employment Referral Conspiracy Involving Chinese Restaurant Industry. January 30, 2014.
[145] (U) Drug Enforcement Administration. United States: Areas of Influence of Major Mexican Transnational Criminal Organizations. July 2015. https://www.dea.gov/docs/dir06515.pdf
[146] (U) Federal Bureau of Investigation. Two Mexican Citizens Face Mandatory Life in Federal Prison After Jury Convicts Them on Federal Charges Related to May 2013 Murder of a Southlake, Texas, Man. May 13, 2016. https://www.justice.gov/usao-ndtx/pr/two-mexican-citizens-face-mandatory-life-federal-prison-after-jury-convicts-them
[147] (U) Worldwide Threat Assessment of the U.S. Intelligence Community. Senate Armed Services Committee. James R. Clapper – Director of National Intelligence. February 9, 2016.
[148] (U) Drug Enforcement Administration. 2015 National Drug Threat Assessment Summary. October 2015. https://www.dea.gov/docs/2015%20NDTA%20Report.pdf
[149] (U) Office of National Drug Control Policy. "Drug Trafficking Across the Southwest Border and Oversight of U.S. Counterdrug Assistance to Mexico" November 17, 2015. https://www.whitehouse.gov/sites/default/files/ondcp/OLA/ondcp_statement_for_nov_17_senate_drug_caucus_mexico_hearing_--_final.pdf
[150] (U) Drug Enforcement Administration. DEA Releases 2016 National Heroin Threat Assessment Summary. June 27, 2016. https://www.dea.gov/divisions/hq/2016/hq062716.shtml
[151]Texas DPS. Texas Border Security Dashboard. July 15, 2015, http://dps.texas.gov/PublicInformation/documents/borderSecDshbrd20150715.pdf
[152] (U) Drug price data is calculated based on the 2014 U.S. National Drug Control Strategy Data Supplement, which includes DEA STRIDE data from 2012 in Tables 66, 67, 68, and 69. This calculation of the retail street price of illegal drugs uses the "Purchases of 10 grams or less" price point multiplied by the "Seizures greater than 100 grams" purity percentage, with the exception of marijuana, for which no purity or potency adjustment is made. http://www.whitehouse.gov/sites/default/files/ondcp/policy-and-research/ndcs_data_supplement_2014.pdf
[153] Operation Secure Texas Incident Log.
[154] Operation Secure Texas Incident Log.
[155] Operation Strong Safety Incident Log.
[156] (U) Texas Department of Public Safety. "Assessing the Threat of Human Trafficking in Texas." March 2014.
[157] (U) United States Border Patrol. Total illegal aliens apprehensions by fiscal year. https://www.cbp.gov/sites/default/files/documents/BP%20Total%20Apps%2C%20Mexico%2C%20OTM%20FY2000-FY2015.pdf
[158] (U) Texas Department of Public Safety, Texas Gang Intelligence Index, data query 2016.

[159] (U) United States Attorney's Office: Southern District of Texas. Two Head to Prison for Committing Murder on Federal Land. April 29, 2016.
[160] (U) "Verdict handed down in machete slaying by MS-13 gang members." Houston Chronicle. June 23, 2016. http://www.chron.com/news/houston-texas/article/Verdict-handed-down-in-machete-gang-slaying-8321037.php
[161] Texas Criminal Alien Arrest Data. https://www.dps.texas.gov/administration/crime_records/pages/txCriminalAlienStatistics.htm
[162](U) Lovett, Ian et. al. "U.C.L.A. Shooting Was Murder-Suicide." *The New York Times*. 1 June 2016. http://www.nytimes.com/2016/06/02/us/ucla-shooting.html?_r=0
[163] *Ibid.*
[164](U) Hamilton, Matt et. al. "For UCLA Shooter Mainak Sarkar, Sudden Rage After Years Of Intense Academic Studies." *Los Angeles Times*. 3 June 2016. http://www.latimes.com/local/lanow/la-me-la-mainak-sarkar-ucla-shooter-20160602-snap-story.html
[165] (U) Honan, Edith. "Al Shabaab kills at least 147 at Kenyan university; siege ends." *Reuters*. 2 April 2015.
[166] (U) Peralta, Eyder. "Taliban Gunmen Storm School, Kill Dozens In Pakistan". *Associated Press*. Npr.org.
[167] (U) United States Attorney's Office: Southern District of Texas. Law Enforcement Officials Among 15 Charged in Drug Trafficking Conspiracy. May 20, 2016.
[168] (U) "Headless Body Leads to Arrest of Border Patrol Agent." Texas Tribune. July 5, 2016. https://www.texastribune.org/2016/07/05/border-patrol-agent-charged-beheading/
[169] (U) United States Attorney's Office: Southern District of Texas. Border Patrol Agent Pleads Guilty to Harboring Undocumented Aliens. November 17, 2014.
[170] (U) United States Attorney's Office: Southern District of Texas. Former Deputy Admits to Money Laundering. May 12, 2014.
[171] (U) Information received from Texas Department of Transportation. April 2016.
[172] (U) Information received from Texas Department of Public Safety - Driver License Division. January 2017.
[173] (U) Information received from Texas Department of Motor Vehicles. April 2016.
[174] (U) Information received from Texas Department of Motor Vehicles – Statewide Registrations by Vehicle Type CY 1994-2014. October 2015
[175] (U) Information received from U.S. Department of Transportation. May 2016.
[176] (U) Information received from Texas Department of Transportation CRIS database. May 4, 2016.
[177] (U) Information received from Texas Department of Transportation CRIS database. May 11, 2016.
[178] (U) Ibid.
[179] (U) Ibid.
[180] (U) Texas Penal Code Title 10. Offenses Against Public Health, Safety, and Morals. Chapter 49. Intoxication and Alcoholic Beverage Offenses.
[181] (U) Information from Texas Department of Transportation. Underage Drinking and Driving. http://www.txdot.gov/driver/sober-safe/underage-drinking.html
[182] (U) National Highway Traffic Safety Administration. Facts and Statistics. Distraction.gov.
[183] (U) Texas Department of Transportation. Talk. Text. Crash. – Distracted Driver Campaign. 2015.
[184] (U) Texas Department of Transportation. Press Release: TxDOT Hosts Distracted Driving Summit To Educate Business Leaders About Risks of Not Having Employee Safe-Driving Policies. June 17, 2014.
[185] (U) Information received from Texas Department of Transportation CRIS database. May 4, 2016.
[186] (U) Texas Department of Transportation. Cell Phone Ordinances. 2015
[187] (U) Information received from Texas A&M Transportation Institute. Talk. Text. Crash. Campaign launches statewide. 2013.
[188] (U) Information received from Texas Transportation Code 545.15. February 2016.
[189] (U) Information received from Texas Department of Transportation CRIS database. May 12, 2016.
[190] (U) Information received from the National Safety Commission – Mason Dixon Polling & Research
[191] (U) Texas A&M Transportation Institute – The Texas Move Over Act: Drive Knowledge, Understanding, and Compliance
[192] (U) Information received from National Highway Traffic Administration. 2015.
[193] (U) Information received from Texas Department of Transportation CRIS database. May 9, 2016.
[194] (U) Information received from Texas Transportation Code 550.021. March 2016.
[195] (U) Information received from Texas Department of Transportation CRIS database. May 9, 2016.

[196] (U) Center for Transportation Research at The University of Texas at Austin. "Impacts of energy development on the Texas transportation system infrastructure." October 2011
[197] (U) Railroad Commission of Texas. http://www.rrc.state.tx.us/permianbasin/index.php
[198] (U) Information received from the Texas Railroad Commission. October 13, 2015.
[199] (U) Railroad Commission of Texas. Texas Permian Basin Drilling Permits Issued 2006 through 2015.
[200] (U) Information received from the U.S. Energy Information Administration. May, 2016.
[201] (U) Information received from the Baker Hughes North American Rig Count. May, 2016.
[202] (U) Railroad Commission of Texas. Texas Permian Basin Drilling Permits Issued 2006 through March 2016. http://www.rrc.state.tx.us/media/25374/permianbasindrillingpermitsissued.pdf
[203] (U) Information received from the Texas Department of Transportation CRIS database. May 4, 2016.
[204] (U) Railroad Commission of Texas. http://www.rrc.state.tx.us/eagleford/index.php
[205] (U) Railroad Commission of Texas. Texas Eagle Ford Shale Drilling Permits Issued http://www.rrc.state.tx.us/media/8675/eaglefordproduction_drillingpermits_issued.pdf
[206] (U) Information received from Texas Department of Transportation. May 4, 2016.
[207] (U) Texas Division of Emergency Management. January 2015.
[208] (U) State of Texas Hazard Mitigation Plan. 2013 Update.
[209] (U) National Flood Insurance Program. https://www.floodsmart.gov/floodsmart/pdfs/FS_FloodRisksFloodAfterFire.pdf
[210] (U) National Weather Service.
[211] (U) "Central Texas Drought Resilience Assessment Report." US Department of Homeland Security. August 2016.
[212] (U) "TribPedia: The Texas-Mexico border," The Texas Tribune, Tribpedia: Texas-Mexico Border, https://www.texastribune.org/tribpedia/texas-mexico-border/
[213] Centers for Disease Control and Prevention (CDC). Online database: Division of Vector-Borne Diseases. April 2, 2016. Retrieved from http://www.cdc.gov/ncezid/dvbd/
[214] (U) University of Texas at Austin. Interactive media: Texas Arbovirus Risk Map. Retrieved from http://arbovirusrisk.org/#/texas
[215] Texas Department of State Health Services (DSHS). Online database: DSHS Arbovirus Weekly Activity Reports. September 13, 2016. Retrieved from http://www.dshs.texas.gov/idcu/disease/arboviral/westNile/reports/weekly/
[216] Lillibridge, et al. "The 2002 Introduction of West Nile Virus into Harris County, Texas, an Area Historically Endemic for St. Louis Encephalitis." February 24, 2004. Retrieved from http://www.ajtmh.org/content/70/6/676.full.pdf+html
[217] Nolan, M.S., Schuemann, J., & Murray, K.O. "West Nile Virus Infection Among Humans, Texas, USA, 2002-2011." January 2013. Retrieved from http://wwwnc.cdc.gov/eid/article/19/1/12-1135_article
[218] Murray, et al. "West Nile Virus, Texas, USA, 2012." Retrieved from https://wwwnc.cdc.gov/eid/article/19/11/pdfs/13-0768.pdf
[219] CDC. "Symptoms and Treatment." February 12, 2015. Retrieved from http://www.cdc.gov/westnile/symptoms/index.html
[220] Ibid.
[221] CDC. "Symptoms and Treatment." November 16, 2009. Retrieved from http://www.cdc.gov/sle/technical/symptoms.html
[222] CDC. "Symptoms and Treatment." November 9, 2009. Retrieved from http://www.cdc.gov/sle/technical/transmission.html
[223] Texas DSHS. "DSHS Announces First Texas-Acquired Chikungunya Case." May 31, 2016. Retrieved from http://www.dshs.texas.gov/news/releases/2016/20160531.aspx
[224] CDC. "Chikungunya Virus." November 16, 2015. Retrieved from http://www.cdc.gov/chikungunya/
[225] CDC. "Dengue." January 19, 2016. Retrieved from http://www.cdc.gov/dengue/
[226] Texas DSHS. "Zika in Texas." Retrieved from http://www.texaszika.org/
[227] CDC. "Viral Hemorrhagic Fevers (VHFs)." January 29, 2014. Retrieved from http://www.cdc.gov/vhf/index.html
[228] Ibid.
[229] CDC. "Ebola (Ebola Virus Disease): Transmission." July 22, 2015. Retrieved from http://www.cdc.gov/vhf/ebola/transmission/index.html
[230] Ibid.

[231] Ibid.
[232] World Health Organization. "Ebola outbreak 2014-2015." Retrieved from http://www.who.int/csr/disease/ebola/en/
[233] World Health Organization. "Ebola outbreak 2014-2015." Retrieved from http://www.who.int/csr/disease/ebola/en/
[234] CDC. "Ebola (Ebola Virus Disease): Cases of Ebola Diagnosed in the United States." December 16, 2014. Retrieved from http://www.cdc.gov/vhf/ebola/outbreaks/2014-west-africa/united-states-imported-case.html
[235] CDC. "Influenza (Flu): Estimating Seasonal Influenza-Associated Deaths in the United States: CDC Study Confirms Variability of Flu." May 26, 2016. Retrieved from http://www.cdc.gov/flu/about/disease/us_flu-related_deaths.htm
[236] CDC. "Influenza (Flu): People at High Risk of Developing Flu–Related Complications." August 25, 2016. Retrieved from http://www.cdc.gov/flu/about/disease/high_risk.htm
[237] Grohskopf, et al. "Prevention and Control of Seasonal Influenza with Vaccines: Recommendations of the Advisory Committee on Immunization Practices – United States, 2016-17 Influenza Season." August 26, 2016. Retrieved from http://www.cdc.gov/mmwr/volumes/65/rr/rr6505a1.htm
[238] CDC. "Middle East Respiratory Syndrome (MERS): Frequently Asked Questions and Answers." July 13, 2016. Retrieved from https://www.cdc.gov/coronavirus/mers/faq.html
[239] CDC. "Middle East Respiratory Syndrome (MERS): MERS in the U.S." July 13, 2016. Retrieved from http://www.cdc.gov/coronavirus/mers/us.html
[240] CDC. "Tuberculosis (TB)." May 6, 2016. Retrieved from http://www.cdc.gov/tb/default.htm
[241] CDC. "Tuberculosis (TB): Data and Statistics." Retrieved from http://www.cdc.gov/tb/statistics/default.htm
[242] Wilson, J. "More than 700 infants exposed to TB at Texas hospital." September 22, 2014. Retrieved from http://www.cnn.com/2014/09/22/health/infants-tb-texas/index.html
[243] Texas DSHS. "TB Statistics." August 3, 2016. Retrieved from https://www.dshs.texas.gov/idcu/disease/tb/statistics/
[244] CDC. "Estimates of Foodborne Illness in the United States: Burden of Foodborne Illness: Findings." July 15, 2016. Retrieved from http://www.cdc.gov/foodborneburden/2011-foodborne-estimates.html
[245] Texas DSHS. "Salmonellosis." August 26, 2016. Retrieved from https://www.dshs.texas.gov/IDCU/disease/salmonellosis/Data/
[246] Kolavic, et al. "An outbreak of Shigella dysenteriae type 2 among laboratory workers due to intentional food contamination." August 6, 1997. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/9244331
[247] (U) Information received from Texas Department of Emergency Management. December 2014.
[248] (U) TLP: White. E-ISAC. "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case" March 18, 2016. http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf
[249] (U) TLP: White. E-ISAC. "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case" March 18, 2016. http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf
[250] (U) Bipartisan Policy Center. "Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat." 2014
[251] (U) TLP: White. E-ISAC. "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case" March 18, 2016. http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf
[252] (U) http://www.ercot.com/about
[253] (U) "Top 9 Things You Didn't Know About America's Power Grid." Energy.gov. November 20, 2014.
[254] *Texas Government Code § 421.001*
[255] (U) Texas Wide Open for Business, Office of the Governor Economic Development and Tourism Business Research.
[256] U.S. Army Corps of Engineers. National Inventory of Dams – Texas. April 2015. http://nid.usace.army.mil/cm_apex/f?p=838:3:0::NO::P3_STATES:TX.
[257] Ibid.
[258] U.S. Energy Information Administration. Texas – State Profile and Energy Estimates. January 21, 2016. http://www.eia.gov/state/analysis.cfm?sid=TX.
[259] (U) U.S Army Corps of Engineers, National Inventory of Dams – Texas.
[260] (U) "Latest on flooding: No Longer Threat of Texas Dam Breaking." May 27, 2015. http://lubbockonline.com/filed-online/2015-05-27/latest-flooding-no-longer-threat-texas-dam-breaking#

[261] (U) Barer. David. "Bastrop State Park dam failure highlights safety." KXAN News. May 26, 2015. http://kxan.com/2015/05/26/bastrop-state-park-dam-failure-highlights-safety/
[262] (U) Getschow, George. "The Dam Called Trouble." Dallas Morning News. December 12, 2015. http://interactives.dallasnews.com/2015/lewisville-dam/
[263] (U) Borrello, Stevie. "Extremely High Risk Dams a Concern Amid Historic Houston Floods." ABCNews. April 20, 2016. http://abcnews.go.com/US/extremely-high-risk-dams-concern-amid-historic-houston/story?id=38553007.
[264] (U) Department of Homeland Security. Emergency Services Sector. https://www.dhs.gov/emergency-services-sector. Accessed on July 27, 2016.
[265] Texas A&M Forest Service. Fire Department Directory. http://tfsfrp.tamu.edu/FDD/directory/. Accessed July 27, 2016.
[266] Texas Division of Emergency Management. Texas Emergency Management Executive Guide, 2015. January 4, 2016. https://www.txdps.state.tx.us/dem/GrantsResources/execGuide.pdf.
[267] Texas Department of State Health Services. Texas Trauma Facilities. https://www.dshs.texas.gov/emstraumasystems/etrahosp.shtm. Last updated July 11, 2016.
[268] Texas Hospitals Association. Hospital Information. http://www.tha.org/Services/Consumer-Information/Hospital-Information. Accessed on July 27, 2016.
[269] US Energy Information Agency, State Profile and Energy Estimates, July 2016.
[270] Texas Department of Insurance, 2015 Annual Report
[271] Texas Department of Banking Agency Profile June 2016
[272] Texas Facilities Commission. Planning and Real Estate Management. http://www.tfc.state.tx.us/divisions/facilities/prog/planning/. Accessed on July 27, 2016.
[273] Ibid.
[274] Texas Education Agency. Pocket Edition State Overview, 2014-2015. http://tea.texas.gov/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=25769825081&libID=25769825178. Accessed on July 27, 2016.
[275] Texas Department of Criminal Justice. Press Release: Executive Director Announces His Retirement. April 15, 2016. https://www.tdcj.state.tx.us/documents/Executive_Director_Announces_His_Retirement.pdf.
[276] Texas Department of Information Resources
[277] Texas Association of Manufacturers. About – Manufacturing Matters. http://manufacturetexas.org/manufacturing-matters. Accessed July 27, 2016.
[278] Diagne, Adji Fatou. U.S. Department of Commerce. Made in America: Computer and Electronic Products. http://webcache.googleusercontent.com/search?q=cache:adwSr-K4od8J:www.esa.doc.gov/sites/default/files/made-in-america-computer-and-electronic-products.pdf+&cd=5&hl=en&ct=clnk&gl=us. Accessed July 27, 2016.
[279] U.S. Geological Survey. 2010 – 2011 Minerals Yearbook: Texas. June 2015. http://minerals.usgs.gov/minerals/pubs/state/2010_11/myb2-2010_11-tx.pdf.
[280] http://www.nrc.gov/about-nrc/state-tribal/agreement-states.html

[281] http://www.energy.gov/sites/prod/files/2016/09/f33/TX_Energy%20Sector%20Risk%20Profile.pdf

[282] http://www.eia.gov/uranium/production/annual/pdf/dupr.pdf

[283] Texas Health and Human Services Commission. 2014-2015 Consolidated Budget. http://www.hhsc.state.tx.us/about_hhsc/finance/2014-2015.pdf. Accessed on July 28, 2016.
[284] Bureau of Transportation Statistics, 2015
[285] Texas Department of Transportation, Texas Transportation Plan 2040